CONSUMER DATA PRIVACY POSTMORTEM OR: HOW I LEARNED TO STOP WORRYING AND LOVE BIG TECH

*Jonathan Kaplan**

"If you are not paying for it, you're not the customer; you're the product being sold."

-Andrew Lewis[1]

INTRODUCTION

The roots of mass data collection that pervade the modern internet can be traced back to what critics have called the internet's "original sin"—the decision to monetize online services through advertising rather than subscriptions.[2] Beginning with a modest $30,000 AT&T banner ad placement in 1994,[3] web companies embraced a model of providing free services while monetizing users' attention and the growing value of their digital real estate with advertisements.[4] Google evolved this model even further by being the first to recognize the value of surplus behavioral data points generated through website interactions, commonly called data exhaust,[5] successfully leveraging this historical user data to optimize both services and advertising effectiveness on its way to becoming the multi-trillion-dollar market leader.[6] This strategy became the template for the modern internet, with companies like Meta, Amazon, and Netflix following suit in building platforms that exchange free services for consumer data and attention.[7] More broadly, the modern digital economy has grown dependent

*Jonathan Kaplan, J.D. Candidate, University of Louisville Louis D. Brandeis School of Law, 2026; M.S.B.A., University of Louisville, 2019; B.A., Psychology, University of Louisville, 2016. I am grateful to the editors of the University of Louisville Law Review for their thoughtful feedback and careful editing. Special thanks to my wife, Whitney, for her resolute support throughout this process.

[1] Andrew Lewis (@andlewis), X (Sep. 13, 2010, at 09:01 ET), https://x.com/andlewis/status/24380177712 [https://perma.cc/9PK9-JGN5].

[2] *See Pop-Up Ad Man 'Fesses to an Internet 'Sin'—But Hopes to Fix It*, NPR (Aug. 18, 2014, at 16:16 ET), https://www.npr.org/2014/08/18/341409795/pop-up-ad-man-fesses-to-an-internet-sin-but-hopes-to-fix-it [https://perma.cc/8Y9N-RRPS].

[3] Ryan Singel, *Oct. 27, 1994: Web Gives Birth to Banner Ads*, WIRED (Oct. 27, 2010, at 07:00 ET), https://www.wired.com/2010/10/1027hotwired-banner-ads/ [https://perma.cc/J87J-D6NJ].

[4] *See id.*

[5] *How Google Discovered the Value of Surveillance*, LONGREADS (Sep. 5, 2019), https://longreads.com/2019/09/05/how-google-discovered-the-value-of-surveillance/ [https://perma.cc/D7JS-ZNQX].

[6] *See id.*

[7] *See* Samuel Chapman, *Big-Tech Companies Selling Data to Third Parties in 2026*, PRIVACYJOURNAL.NET (Dec. 19, 2024), https://www.privacyjournal.net/big-tech-data-collection/ [https://perma.cc/NR36-N273].

on this model, with businesses requiring consumer data for strategic decision-making and to maintain market competitiveness.[8]

This commodification of consumer data and attention has produced an explosion in data collection. In 2023, among the 5.35 billion internet users worldwide, the average person generated an estimated 75.3GB of consumer data per day.[9] To help put this volume in perspective, by 2025, global data creation is projected to reach 181 zettabytes—equivalent to 1 trillion gigabytes[10]—representing an increase of over 8,950% from 2010.[11] This exponential growth is expected to persist as computing power advances, thanks to Moore's Law[12], and as modern daily life continues to produce a steady stream of consumer data. Every digital interaction—whether checking email, browsing social media, tracking fitness, using smartphones while traveling, or adjusting smart home settings—generates consumer data points.[13] While companies collect this data directly from consumers, much of it is routinely resold to third parties through active secondary markets.[14] Several years ago, Apple Chief Executive Officer (CEO) Tim Cook aptly referred to this advertising-based ecosystem as the data-industrial complex.[15]

In recent years, there has been a growing public awareness of these processes thanks to events like the Cambridge Analytica scandal,[16] perpetual data breaches that exposed billions of consumer records in 2024,[17] and the

---

[8] *See* Heidi Bullock, *Data Differentiation: Why Customer Data Is a Modern Organization's Real Competitive Advantage*, FORBES (Oct. 2, 2024, at 07:15 ET), https://www.forbes.com/councils/forbescommunicationscouncil/2024/10/02/data-differentiation-why-customer-data-is-a-modern-organizations-real-competitive-advantage/ [https://perma.cc/9SXT-SMFJ] (examining how businesses across sectors have become reliant on consumer data analytics to compete).

[9] *Breaking Down the Numbers: How Much Data Does the World Create Daily in 2024?*, EDGE DELTA (Mar. 11, 2024) https://edgedelta.com/company/blog/how-much-data-is-created-per-day [https://perma.cc/U7YF-SKLK].

[10] *See* Petroc Taylor, *Volume of Data or Information Created, Captured, Copied, and Consumed Worldwide from 2010 to 2025*, STATISTA (Nov. 19, 2025), https://www.statista.com/statistics/871513/worldwide-data-created/ [https://perma.cc/539F-5D7N].

[11] *See id.*

[12] *See* Max Roser, Hannah Ritchie & Edouard Mathieu, *What is Moore's Law?*, OUR WORLD IN DATA (Mar. 28, 2023), https://ourworldindata.org/moores-law [https://perma.cc/RR2N-L4HZ] (explaining that Moore's Law states that the amount of transistors on a computer chip roughly doubles every two years, facilitating companies' ability to capture, store, and monetize greater amounts of consumer data).

[13] *See* Allen Bernard, *What Defines Customer Data Today?*, CMSWIRE (June 16, 2023), https://www.cmswire.com/digital-experience/what-defines-customer-data-today/ [https://perma.cc/A9ES-HE8H].

[14] *See* Robert Sheldon, *What Is a Data Broker (Information Broker)?*, TECHTARGET (Feb. 26, 2024), https://www.techtarget.com/whatis/definition/data-broker-information-broker [https://perma.cc/BYE7-Z4BS].

[15] Zach Baron, *Tim Cook on Why it's Time to Fight the "Data-Industrial Complex,"* GQ (Jan. 28, 2021), https://www.gq.com/story/apple-ceo-tim-cook-privacy-initiative [https://perma.cc/75PL-QGHQ].

[16] *See* Geoffrey Garrett, *The Politics of Data Privacy in a Post-Cambridge Analytica World*, WHARTON MAG. (May 8, 2018), https://magazine.wharton.upenn.edu/digital/the-politics-of-data-privacy-in-a-post-cambridge-analytica-world/ [https://perma.cc/RNL8-YUKW].

[17] *See* Joanna Krysińska, *Biggest Data Breaches of 2024*, NORDLAYER, (Dec. 16, 2024), https://nordlayer.com/blog/data-breaches-in-2024/ [https://perma.cc/Y2EY-6SBW].

popular Netflix documentary *The Social Dilemma*.[18] Most consumers now broadly understand they are trading personal data for free services,[19] yet despite the growing recognition of this underlying bargain, the public remains largely ignorant as to what, who, and how data is being captured from their daily interactions with internet-connected devices, and ultimately, what is being done with it.[20]

Enabling this rapid growth of the digital economy is a weak and limited regulatory environment predicated on the Notice and Consent framework.[21] Businesses accurately assert that their data collection practices are legally authorized with the requisite user consent as part of the bargained-for exchange of data-subsidized services.[22] However, in practice, these Privacy Policies are typically buried within Terms of Service agreements, presented through clickwrap or browsewrap interfaces,[23] and written in deliberately complex language.[24] For example, when Forbes commissioned seven privacy attorneys to review the iTunes privacy policy, they reportedly were still unable to decipher it after seven days.[25] Critics highlight how the Notice and Consent framework ironically fails at its core purpose—it neither obtains affirmative user consent nor provides genuine notice, yet remains legally sufficient to justify widespread collection of consumer data.[26]

With many consumers feeling like they lack choice or control over their data, bipartisan support has grown for stronger data privacy laws.[27] Yet despite this support, the federal government has been wholly unable to pass a federal law, allowing a patchwork of state laws to emerge in its place.[28] These state laws are generally modeled after the European Union's (EU)

---

[18] *See* Toni Stanger, *Netflix's 'The Social Dilemma' Looks at How Social Media Is Changing the Way We Think*, MEDIUM (Sep. 22, 2020), https://tonistanger.medium.com/netflixs-the-social-dilemma-looks-at-how-social-media-is-changing-the-way-we-think-136ba62319fb [https://perma.cc/AFQ6-HANS].

[19] *See* Timothy Morey, Theodore "Theo" Forbath & Allison Schoop, *Customer Data: Designing for Transparency and Trust*, HARV. BUS. REV., May 2015, at 96, https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust [https://perma.cc/5GFJ-7HKY?type=image].

[20] *See id.*

[21] *See* discussion *infra* Section II.B.1 (analyzing fundamental failures of Notice and Consent framework).

[22] *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 77 (2013) (discussing the "free" services model where users exchange personal data for access).

[23] *See Clickwrap vs. Browsewrap: What's the Difference?*, IRONCLAD (Jan. 4, 2022), https://ironcladapp.com/journal/contracts/clickwrap-vs-browsewrap/ [https://perma.cc/3BPS-QDXY] (explaining that clickwrap agreements require users to actively indicate agreement, while browsewrap agreements provide access to terms via hyperlink without requiring explicit user action).

[24] *See* discussion *infra* Section II.B.1.

[25] Stuart Lacey, *7 Things You Didn't Know About Your Privacy*, FORBES (Oct. 27, 2014, at 09:05 ET), https://www.forbes.com/sites/theyec/2014/10/27/7-things-you-didnt-know-about-your-privacy/ [https://perma.cc/NE2Q-6SFJ].

[26] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 Harv. L. REV. 1880, 1883–84 (2013) (discussing how notice and consent frameworks often fail to provide meaningful privacy protection despite their legal sufficiency).

[27] *See* discussion *infra* Section II.A.4 (discussing populist support for stronger data privacy regulation).

[28] *See* discussion *infra* Section II.A.3–4.

General Data Protection Regulation (GDPR) structure, which aims to empower consumers with greater control and choice over their data.[29] However, many privacy advocates and legal scholars assert that these laws fall far short of providing effective consumer controls over personal data or of addressing the information and power asymmetries that exist between consumers and the tech giants that make up the data-industrial complex.[30]

What privacy advocates fail to appreciate in their pursuit of a unilateral legal solution is the degree to which tech giants like Alphabet, Amazon, Meta, and Microsoft (Big Tech) have consumers dependent on their free or heavily data-subsidized services.[31] The advertising-based business models of these platforms are engineered to attract widespread user adoption and addictively retain attention so that consumer data can be reliably collected and attention auctioned to the highest-bidding advertiser.[32] Moreover, the American public has generally grown dependent on free access to these cutting-edge technologies. A 2019 study found roughly 80 percent of respondents preferred Meta and Alphabet collect less data, but a majority retracted their position when asked if they would pay for that benefit,[33] demonstrating consumers' unwillingness to pay for privacy-forward alternatives. Confounding this situation is the recent addition of massive investments into Artificial Intelligence (AI) infrastructure, which looks likely to accelerate this dynamic.[34]

This Note will divert from the pro-privacy arguments consistently made in the idealistic academic echo chambers, divorced from reality. Going beyond the surface-level presentation of this issue as a zero-sum game where big business is pitted against our collective right to privacy to embrace a more complex and nuanced understanding of this issue: where modern life demands the constant use of technology, where most are dependent on, and many addicted to their devices, where an insatiable public hunger for free cutting-edge technology is aligned rather than conflicted with the sacrifice of personal privacy.[35] This Note argues for the acceptance and embrace of weak consumer data privacy laws as the fair-market cost for the free online services consumers demand.[36]

---

[29] *See* discussion *infra* Section II.A.
[30] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585–87 (2014) (analyzing the limitations of current U.S. privacy regulatory framework).
[31] *See* discussion *infra* Section II.C.1.
[32] *See* discussion *infra* Section II.C.1.
[33] Daniel Castro & Michael McLaughlin, *Survey: Few Americans Willing to Pay for Privacy*, CTR. FOR DATA INNOVATION (Jan. 16, 2019), https://datainnovation.org/2019/01/survey-few-americans-willing-to-pay-for-privacy/ [https://perma.cc/A3EW-VBDH].
[34] *See* discussion *infra* Section I.D.2.
[35] *See* discussion *infra* Section II.C.1.
[36] *See* discussion *infra* Section III.A.

To better understand this dynamic, Part I provides a foundational background of how consumer data flows through the modern digital economy, exploring several key questions about the value of consumer data, types and methods of data collection, the entities involved in gathering this data, and its subsequent applications. Part II continues with a comprehensive analysis of the current state of consumer data privacy law and the fundamental issues that plague it, beginning with a broad examination of the regulatory landscape—from early Federal Trade Commission (FTC) led enforcement to subject-specific privacy laws, to the recent emerging patchwork of comprehensive regulations and failed attempts to pass a federal law. The analysis proceeds by examining three categories of systemic issues that plague these regulatory frameworks: the structural failures of Notice and Consent, challenges with enforcement and compliance, and significant gaps in secondary-market oversight. Part II concludes by examining the social, political, and market forces that make the passage of a robust federal privacy law impractical for the foreseeable future. Finally, Part III advocates for acceptance of diminished personal privacy and the current weak regulatory environment as the logical trade-off for the modern digital economy while simultaneously proposing an expanded federal framework of liability to address substantial harms resulting from data misuse.

I. CONSUMER DATA AND THE MODERN DIGITAL ECONOMY

Part I provides a comprehensive background of how consumer data flows through the modern digital economy, from its initial collection through its ultimate use in increasingly complex applications. Beginning with why businesses value consumer data as a rapidly depreciating but essential asset, the discussion progresses through data types and collection processes, then identifies the key entities involved in data collection—from Big Tech platforms to individual businesses—before exploring both documented and emerging applications of consumer data. This background context of data collection practices and market dynamics proves essential for the subsequent analysis of regulatory frameworks and their deficiencies in addressing the challenges of the modern digital economy.

A. The Strategic Value of Consumer Data

Understanding consumer data's place in the modern digital economy requires first contextualizing this data's underlying economic value. While businesses collecting customer information is nothing new, the internet has dramatically accelerated both the variety and volume of data that companies

capture and process.[37] This technological shift has created a hyper-competitive environment where reliable access to consumer data has become a prerequisite to successfully running a modern business.[38] Moreover, as data breaches become increasingly common and costly—with the average breach now costing companies $4.4 million in direct expenses and immeasurable reputational damage—maintaining robust data security practices has become an essential aspect of protecting this valuable business asset.[39]

Adding further complexity to this dynamic is that businesses view consumer data as an intangible asset that is rapidly and perpetually depreciating.[40] Unlike other intangible assets such as copyrights and patents, the accuracy and value of consumer data degrades immediately after collection.[41] One study found that customer data degrades at an annual rate of 22 percent, as things like home and internet protocol (IP) addresses change and attitudes and life circumstances shift.[42] This depreciation puts businesses constantly at risk of basing strategic decisions on stale information, as no executive wants to erroneously base a product pricing or marketing strategy decision on an assumption.[43] Consequently, many companies feel compelled to continuously purchase or rent fresh consumer data to maintain accurate insights, helping fuel the overall market demand for personal information.[44]

B. Types and Methods of Consumer Data Collection

The competitive need for accurate data has led businesses to capture a wide array of information, including identity, demographic, psychographic, behavioral, biometric, and technical data.[45] Identity data—foundational to digital tracking—encompasses both traditional identifiers, such as names and social security numbers, as well as digital identifiers, like email addresses,

---

[37] *See Consumer Data: Unveiling the Power of Market Insights*, NIELSENIQ, https://nielseniq.com/global/en/info/consumer-data/ [https://perma.cc/95X3-E8EN] (last visited Sep. 20, 2024).
[38] *Id.*
[39] IBM, *Cost of a Data Breach Report* 2025, https://www.ibm.com/reports/data-breach [https://perma.cc/ANC6-DL4D].
[40] *See* Marc Smith, *Unlocking the Hidden Value of Data as an Asset*, TEKSYSTEMS (Dec. 20, 2023), https://www.teksystems.com/en/insights/article/data-as-an-asset [https://perma.cc/MZC9-Z6BX].
[41] Vinny Maurici, *Understanding Data Decay: Causes, Impact, and How to Mitigate It*, OBJECT EDGE (Oct. 30, 2025), https://www.objectedge.com/blog/understanding-the-phenomenon-also-known-as-data-decay [https://perma.cc/U7LG-46XL].
[42] *Id.*
[43] *See How Data Chaos Undermines Your Business Success*, DATA SLEEK (Sep. 30, 2024), https://data-sleek.com/blog/how-data-chaos-undermines-your-business-success/ [https://perma.cc/6PSN-29LK].
[44] *See* Anja Lambrecht & Catherine E. Tucker, *Can Big Data Protect a Firm from Competition?,* 17 COMPETITION POL'Y INT'L 258 (2017).
[45] *See* Lauren Saalmuller, *Understanding Customer Data: Types, and How to Collect and Segment*, SIMON AI (Oct. 18, 2022), https://www.simondata.com/blog-posts/understanding-customer-data-types-and-how-to-collect-and-segment [https://perma.cc/LPL6-VBCK].

cookie identifiers (IDs), device IDs, and IP addresses.[46] These digital identifiers allow companies to connect consumer behavior across platforms and devices, often beyond the user's conscious awareness.[47]

The combination of demographic, psychographic, and behavioral data gives businesses an unprecedented look into consumer preferences and habits.[48] While demographic data collection—including characteristics like age, gender, and income—predates the internet,[49] modern methods have evolved from periodic collection to real-time profiling through digital interactions.[50] Psychographic data—defined as consumers' values, attitudes, and personality traits—has also become more prominent through website analytics and social media platforms.[51] When combined with online behavioral data—including browsing patterns, app usage, purchase history, and platform engagement metrics—[52] and offline geolocational data generated from smartphones' GPS, IP addresses, and Wi-Fi triangulation,[53] businesses can create comprehensive profiles that connect the dots between online and offline behavior.[54]

The emergence of biometric data collection through Internet-of-Things (IoT) devices and wearable technology creates unique challenges due to its sensitive and immutable nature, as many biometric identifiers cannot be changed if compromised.[55] Finally, while seemingly innocuous, technical data acts as the connective tissue of the modern data ecosystem, allowing companies to stitch various unrelated data points into cohesive consumer

---

[46] *See What is Identity Data? Definition, Uses & Datasets to Buy in 2024*, DATARADE (Sep. 20, 2024), https://datarade.ai/data-categories/identity-data [https://perma.cc/ERQ4-EKEK].

[47] *See Cross Site Tracking: Addressing Cross Site Tracking in Modern Cookie Policies*, FASTERCAPITAL (Apr. 6, 2025), https://www.fastercapital.com/content/Cross-Site-Tracking--Addressing-Cross-Site-Tracking-in-Modern-Cookie-Policies.html [https://perma.cc/AAJ2-2YLU].

[48] *See* Saalmuller, *supra* note 45.

[49] *See Demographic Surveys History*, U.S. CENSUS BUREAU (Sep. 3, 2024), https://www.census.gov/about/history/historical-censuses-and-surveys/census-programs-surveys/demographic.html [https://perma.cc/YF8V-XBGH] (discussing the history of the U.S. Census Bureau's collection of demographic data).

[50] Bella Williams, *Top 8 Demographic Research Tools,* INSIGHT7, https://insight7.io/top-8-demographic-research-tools/ [https://perma.cc/B6E8-N22X] (last visited Jan. 31, 2025).

[51] *Ultimate Guide to Psychographic Data*, MAILCHIMP, https://mailchimp.com/resources/pyschographic-data/ [https://perma.cc/WER4-34JT] (last visited Sep. 20, 2024).

[52] Jackelyn Gill, *User Behavioral Data: A Competitive Edge Explained,* COVEO: BLOG (June 25, 2024), https://www.coveo.com/blog/what-is-behavioral-data/ [https://perma.cc/FU9R-ZFDF].

[53] *Geolocation Data*, SECURITI, https://securiti.ai/glossary/geolocation-data/ [https://perma.cc/TGF2-YN46] (last visited Sep. 20, 2024).

[54] OWOX, *How to Integrate Online and Offline Data for Omnichannel Retailing: Why and How to Connect Customer Touchpoints*, MEDIUM (July 12, 2024), https://medium.owox.com/how-to-integrate-online-and-offline-data-for-omnichannel-retailing-why-and-how-to-connect-customer-a45da61a70f4 [https://perma.cc/3753-Q5PZ].

[55] *See* Wencheng Yang et al., *Biometrics for Internet-of-Things Security: A Review*, 21 Sensors 6163 (2021), https://pmc.ncbi.nlm.nih.gov/articles/PMC8472874/pdf/sensors-21-06163.pdf [https://perma.cc/QBN5-T4MQ].

profiles via cross-device tracking.[56] Armed with this asymmetry of insight into consumers' habits and demonstrated preferences, businesses can move beyond descriptive and into predictive analysis, enabling increasingly invasive targeting and behavioral modification strategies that raise novel privacy concerns.[57]

To capture this data, businesses use several mechanisms, none more widespread than cookies.[58] While first-party cookies that track user interactions within individual websites raise limited privacy concerns, third-party cookies that enable comprehensive cross-site tracking have drawn criticism for violating consumers' reasonable expectations of privacy.[59] This data is commonly aggregated into profiles and made available as marketable segments on advertising exchanges, fueling an active secondary market that operates beyond the scope of consumers' original consent.[60]

Mobile applications are another popular mechanism of data collection, most notably of geolocation data.[61] While some app-tracking does serve legitimate purposes—such as optimizing functionality—most serve to extract more data.[62] Further confounding this dynamic is the prevalence of software development kits (SDKs), as these widely used tools for app development often include hidden functionality that monetizes consumer data by feeding it into the secondary market.[63] Platform tracking—the process by which companies capture profile data voluntarily entered onto their platforms and from interactions with content across their integrated service offerings—is a third major collection mechanism.[64] The "Walled Garden" advertising model, where platform data and consumer access are made exclusively available within their ecosystem, was initially pioneered in

---

[56] *See What Is Cross-Device Tracking?*, ADJUST, https://www.adjust.com/glossary/cross-device-tracking/ [https://perma.cc/MF5L-HCXY] (last visited Sep. 20, 2024) (explaining how cross-device tracking works).

[57] *See* discussion *infra* Section I.D.2.

[58] *See* Griffin LaFleur, *First-Party vs. Third-Party Cookies: What's the Difference?*, TECHTARGET (July 29, 2024), https://www.techtarget.com/searchcustomerexperience/tip/First-party-vs-third-party-cookies-Whats-the-difference [https://perma.cc/T228-8C8N] (discussing that cookies are text files stored on users' devices that enable websites to track browsing activity, maintain login sessions, and collect data about user behavior and preferences across multiple web pages).

[59] *Id.*

[60] *Cookie Segmentation*, OMNICONVERT (Apr. 26, 2025), https://www.omniconvert.com/what-is/cookie-segmentation/ [https://perma.cc/49VG-FZJC].

[61] *See* Jonas Kurzweg, *Mobile App Tracking Tools: A Complete Guide for 2024*, UXCAM (Nov. 7, 2024), https://uxcam.com/blog/mobile-app-tracking-tools/ [https://perma.cc/2QL4-VHPU].

[62] *See id.*

[63] Sara Morrison, *The Hidden Trackers in Your Phone, Explained*, VOX (July 8, 2020, at 10:30 ET), https://www.vox.com/recode/2020/7/8/21311533/sdks-tracking-data-location [https://perma.cc/2HV5-3F8N].

[64] *See* Brock Munro, *What Are Walled Garden in Advertising & Tech?*, PUBLIFT (Dec. 9, 2025), https://www.publift.com/blog/walled-gardens [https://perma.cc/3LU7-2M5G].

the digital sector by companies like Meta and Alphabet[65] but has since become a Big Tech industry standard.[66]

Finally, bidstream data—which is the stream of data associated with every transaction occurring on digital advertising exchanges—creates unique privacy challenges that remain largely unaddressed by current regulatory frameworks.[67] Programmatic advertising, similar to stock market transactions, functions through open exchanges where inventory is auctioned to the highest bidder, with every transaction leaving behind key pieces of consumer data.[68] While most exchanges explicitly prohibit the direct use of this data, industry insiders acknowledge its widespread repackaging and sale, contributing to a shadow market for consumer information collected without any pretense of consent.[69] Collectively, these mechanisms represent the most prolific tracking methods, but this list is by no means exhaustive.[70] The current landscape of data collection is diverse and rapidly evolving, with many practices obscured by complex privacy policies.

C. Key Players in the Data Economy

The data economy consists of a network of organizations that collect consumer information, each with distinct capabilities, motives, and impacts on privacy. Dominating this ecosystem are the Big Tech platforms, whose integrated service offerings enable comprehensive data collection and analysis.[71] Their market dominance shapes the broader privacy landscape. Supporting this is a thriving secondary market driven by data brokers who aggregate and monetize information, while individual businesses increasingly collect customers' first-party data to remain competitive.

1. Big Tech: Integrated Platforms and Market Dominance

---

[65] *Id.*

[66] *See id.*; *see also* Jeremy Goldman, *Netflix Plans New Ad Tech Platform as it Nearly Doubles Ad-Supported Users*, EMARKETER (May 16, 2024), https://www.emarketer.com/content/netflix-nearly-doubles-ad-supported-users-plans-new-ad-tech-platform [https://perma.cc/2836-NP62] (discussing how this practice has expanded across digital sectors to all of Big Tech, with Amazon mining e-commerce interactions to sell sponsored product placement at the top of search results and Netflix planning to integrate this advertising model by 2025).

[67] *See What Is Bidstream Data in Programmatic Advertising?*, BIDSCUBE (July 6, 2023), https://bidscube.com/blog/2023/07/06/what-is-bidstream-data-in-programmatic-advertising/ [https://perma.cc/W49M-VAJC].

[68] *Id.*

[69] *See* Erik Matlick, Opinion, *Are Brands Unknowingly Stealing Bidstream Data?*, ADEXCHANGER (Mar. 14, 2022, at 09:34 ET), https://www.adexchanger.com/data-driven-thinking/are-brands-unknowingly-stealing-bidstream-data/ [https://perma.cc/QF27-KL57].

[70] *See* Saalmuller, *supra* note 45.

[71] *See* David Flower, *The Power of Ecosystems: How Collaboration Fuels Tech*, FORBES (Apr. 14, 2025, 06:15 ET), https://www.forbes.com/councils/forbestechcouncil/2025/04/14/the-power-of-ecosystems-how-collaboration-fuels-tech/ [https://perma.cc/EX5V-EP3L].

All of Big Tech uses some version of the same general business model: attract consumers to their platform with a free or heavily subsidized primary service offering, such as a search engine, social media platform, or e-marketplace.[72] They pair these offerings with complementary services to retain consumer engagement while facilitating systemic data collection across their integrated platforms.[73] Consumers' data and attention are then monetized via digital advertising in integrated platforms owned and operated by these companies.[74] Companies like Alphabet, Meta, and Amazon have all successfully employed some version of this strategy to great effect.[75]

Alphabet provides the best illustration of this strategy through its integrated suite of consumer services.[76] Primarily known for its market-leading search engine, Google,[77] and internet browser, Chrome,[78] which together enable the collection of first-party data directly from users and third-party data through cookies and tools such as Google Ads and Analytics as users navigate the internet.[79] Alphabet has built out a subsequent suite of complementary products that, on its face, create a more holistic customer experience, but in reality, facilitate more data collection opportunities for the company to fuel its advertising business.[80] The company captures professional communications through Gmail, included with their Workspace Services suite,[81] media and interest preferences through YouTube,[82] and

---

[72] *See* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER 64–67 (2019) (describing how major tech companies adopted the model of offering free services to enable data extraction).

[73] *See id.* at 93–96 (analyzing the business model of tech platforms).

[74] *Id.*

[75] *See id.* at 9 (discussing how Alphabet, Meta (then Facebook), and Amazon adapted this business model).

[76] *Id.* at 93–96 (providing detailed analysis of Google's integrated service strategy).

[77] *See Search Engine Market Share Worldwide,* STATCOUNTER GLOBALSTATS, https://gs.statcounter.com/search-engine-market-share [https://perma.cc/ZEY6-NKTU] (last visited Sep. 20, 2024) (showing how Google's search engine has consistently held a ninety percent market share).

[78] *See Browser Market Share Worldwide*, STATCOUNTER GLOBALSTATS, https://gs.statcounter.com/browser-market-share [https://perma.cc/DG44-XMRR] (last visited Sep. 20, 2024) (showing how Google Chrome holds a dominant sixty-five percent worldwide market share).

[79] *How Google Uses Cookies*, GOOGLE, https://policies.google.com/technologies/cookies [https://perma.cc/9MJF-LF5F] (last visited Jan. 31, 2025) (detailing Google's use of first-party and third-party cookies for data collection across its products).

[80] *See* ZUBOFF, *supra* note 72, at 93–96.

[81] *See* Laurel Wamsley, *Google Says it Will No Longer Read Users' Emails to Sell Targeted Ads*, NPR (June 26, 2017, at 17:40 ET), https://www.npr.org/sections/thetwo-way/2017/06/26/534451513/google-says-it-will-no-longer-read-users-emails-to-sell-targeted-ads [https://perma.cc/S2EQ-T6PD] (discussing how Google's Gmail service allowed the company to scan the contents of consumers' emails. This practice was stopped in 2017 as the company pivoted due to bad press, but it illustrates the privacy adverse attitude with which Big Tech operates, enabling Google to stitch together professional and personal data).

[82] *See* Lauren Pabst, *Younger Viewers, Olympics Drive Big Month for YouTube and NBCUniversal in Nielsen's July Media Distributor Gauge*, NIELSEN, (Sep. 3, 2024), https://www.nielsen.com/news-center/2024/younger-viewers-olympics-drive-big-month-for-youtube-and-nbcuniversal-in-nielsens-july-media-distributor-gauge/ [https://perma.cc/TF52-YZZ6] (discussing how YouTube accounts for 10.7% of all TV viewing according to Nielsen).

location data through Maps and Android devices.[83] Each service appears to operate independently but feeds into Alphabet's comprehensive data collection system, which fuels its primary monetization tool: the advertising business.[84] With the recent emergence of artificial intelligence (AI), consumer data now serves an additional purpose as the critical training data for Gemini, Alphabet's AI platform that aims to integrate AI capabilities across these service offerings.[85]

Meta similarly leverages its social media platforms to gather extensive identity, behavioral, and psychographic data.[86] Through Facebook, Instagram, and WhatsApp, the company goes beyond collecting profile information to track content engagement, social connections, and emotional responses.[87] This data is used to create detailed consumer profiles that drive its advertising business.[88] Not wanting to get left behind in the AI race, Meta has also begun leveraging this trove of consumer data to develop its open-source AI model Llama, which it can use to further its consumer engagement and data collection efforts.[89]

Amazon's e-commerce platform illustrates how consumer data collection transcends traditional digital services.[90] Beyond tracking purchase histories, the company monitors browsing patterns, product interactions, and search behaviors to create detailed consumer profiles and trend data.[91] Through services like Prime Video, Whole Foods Market, and IoT devices like Alexa and Ring cameras, Amazon has expanded its data collection far beyond online shopping preferences to provide them with a holistic look into consumers' daily lives.[92] Amazon then uses these insights to optimize the profitability of its marketplace by refining search algorithms and positioning sponsored products[93] while simultaneously developing private label products

---

[83] Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018, at 18:15 ET), https://apnews.com/article/828aefab64d4411bac257a07c1af0ecb [https://perma.cc/MGB9-TPGQ].

[84] *See Alphabet Q2 FY24 Income Statement*, SANKEYART, https://www.sankeyart.com/sankeys/public/28246/ [https://perma.cc/UV33-HHRT] (last visited Jan. 2, 2025).

[85] Ina Fried, *What Google's AI Knows About You*, AXIOS (Nov. 18, 2024), https://www.axios.com/2024/11/18/google-ai-gemini-user-data-training [https://perma.cc/UH6A-NGPD].

[86] *Meta Ads Detailed Targeting*, SAVE MY LEADS: BLOG (Oct. 1, 2024), https://savemyleads.com/blog/other/meta-ads-detailed-targeting [https://perma.cc/2TDX-VN5U].

[87] *See Privacy Policy*, META (Dec. 16, 2025), https://www.facebook.com/privacy/policy [https://perma.cc/5ZYK-CWJG].

[88] *See id.*

[89] Ina Fried, *Meta's AI Feasts on User Data*, AXIOS (Nov. 5, 2024), https://www.axios.com/2024/11/05/meta-ai-user-data-information [https://perma.cc/5MT4-JR4P].

[90] *See* Rachyl Jones, *What Does Amazon Do with Your Data?*, OBSERVER (July 6, 2023, at 12:00 ET), https://observer.com/2023/07/what-does-amazon-do-with-your-data/ [https://perma.cc/RPV7-VH48].

[91] *Id.*

[92] *See id.*

[93] Reilly McDonnell, *Amazon's Search Algorithm: How Does It Work?*, JUMPFLY (Oct. 11, 2023),

that directly compete with third-party sellers on its platform.[94] This expanded window into customers' homes and daily routines further propels the data flywheel that powers Amazon's diverse business empire.[95]

All of Big Tech operates some version of this model, with the primary objective of maintaining "sticky" user experiences to maximize platform engagement, fueling the feedback loop where increased usage generates more data for further targeted advertising.[96] This system has enabled Big Tech to establish significant information asymmetries over both consumers and competitors, which they leverage to dominate their respective markets, develop increasingly addictive products, and generate massive advertising revenue.[97]

2. Data Brokers and the Secondary Market

Data brokers aggregate and repackage first-party and third-party data into marketable segments, often presented as panelized consumer profiles or as subject-specific categories like real estate or politics.[98] Brokers collect data through various methods, including scraping public profiles and purchasing first-party data directly from companies with broad consumer exposure via cookies, profile data, and mobile apps.[99] Much of this occurs beyond the scope of explicit consumer consent, with data often repackaged and sold several times over on an active secondary market.[100] Brokers sell and license this data to everyone, from political campaigns and financial institutions to insurance and healthcare providers;[101] brokers also make it available as rentable targeting segments on advertising exchanges.[102]

Despite a negative reputation,[103] data brokers serve the vital market function of providing businesses with consumer insights needed for strategic

---

https://www.jumpfly.com/blog/amazons-search-algorithm-how-does-it-work/ [https://perma.cc/5UST-V3MG] (describing how Amazon leverages seller and customer data to optimize search rankings and promote its private-label products).

[94] Gadjo Sevilla, *Amazon's Use of Seller Data for Private-Label Business Is Under SEC Scrutiny*, EMARKETER (Apr. 7, 2022), https://www.emarketer.com/content/amazon-s-use-of-seller-data-private-label-business-under-sec-scrutiny [https://perma.cc/ P7VU-4KVG].

[95] *See id.*

[96] *See* PAUL-ADRIEN HYPPOLITE & ANTOINE MICHON, *BIG TECH DOMINANCE (2): A BARRIER TO TECHNOLOGICAL INNOVATION?* (2018), https://www.fondapol.org/app/uploads/2020/06/136-geants-numerique-ii-eng-2019-07-11-w-3.pdf [https://perma.cc/WW7L-UAGR].

[97] *See id.*

[98] Sheldon, *supra* note 14.

[99] *Id.*

[100] Lesley Fair, *What Goes on in the Shadows: FTC Action Against Data Broker Sheds Light on Unfair and Deceptive Sale of Consumer Location Data*, FED. TRADE COMM'N: BUS. BLOG (Jan. 9, 2024), https://www.ftc.gov/business-guidance/blog/2024/01/what-goes-shadows-ftc-action-against-data-broker-sheds-light-unfair-deceptive-sale-consumer-location [https://perma.cc/HMG8-PQJ6].

[101] Chapman, *supra* note 7.

[102] *See id.*

[103] Bhaskar Medhi, *The Dirty World of Data Brokering*, MEDIUM (Mar. 26, 2018),

decision-making.[104] The secondary market's significance is reflected in its size, with a valuation of $252 billion in 2023.[105] It encompasses over 4,000 companies worldwide,[106] including the market leader Experian, which generates $7 billion in annual revenue,[107] and legal research companies like LexisNexis and Westlaw's parent company Thomson Reuters.[108]

Important as they are to the secondary market and overall data ecosystem,[109] the primary focus of privacy regulation remains on the role of Big Tech. Data brokers perform a relatively limited role as data intermediaries compared to Big Tech, which, as platform operators, has end-to-end involvement throughout the consumer data lifecycle.[110]

3. Individual Business: Data Collection Practices

The transition to Web 2.0 in the early 2000s prompted most businesses to establish digital presences that enable consumer data collection primarily using cookies.[111] While customer record-keeping predated the internet,[112] modern customer relationship management (CRM) and website analytics software have dramatically expanded the ability to monitor and analyze consumer behavior.[113] Many companies have extended their data collection reach through mobile apps, leveraging gamified experiences and reward programs to promote engagement and gather more granular behavioral data.[114]

---

https://medium.com/@bhaskarmedhi/this-post-originally-appeared-in-businessline-and-was-co-authored-with-debapratim-purkayastha-e734589643ef [https://perma.cc/9EU4-3WYR].

[104] *See* Sheldon, *supra* note 14.

[105] *Data Broker Market: Global Industry Analysis and Forecast (2025-2032) by Data Category, Data Type, End- User and Region*, MAXIMIZE MKT. RSCH. (Jan. 2025), https://www.maximizemarketresearch.com/market-report/global-data-broker-market/55670/ [https://perma.cc/99TD-Z8ZW].

[106] *What Are Data Brokers – And What Is Your Data Worth? [Infographic],* WEBFX: BLOG, https://www.webfx.com/blog/internet/what-are-data-brokers-and-what-is-your-data-worth-infographic/ [https://perma.cc/ZN92-8RUN] (last visited Sep. 20, 2024).

[107] *Full-Year Results FY24: Another Year of Strong Growth: New Medium-Term Outlook*, EXPERIAN (May 15, 2024, at 07:00 ET), https://www.experianplc.com/newsroom/press-releases/2024/experian-full-year-results-fy24 [https://perma.cc/77E3-47GR].

[108] *See* Sarah Lamdan, *Westlaw, Lexis, Elsevier, and SSRN Belong to Data Brokers: What Does that Mean for Professional Research?*, CORNELL INFO. SCIENCE (Sep. 10, 2021), https://infosci.cornell.edu/content/westlaw-lexis-elsevier-and-ssrn-belong-data-brokers-what-does-mean-professional [https://perma.cc/Q7C3-YD4T].

[109] *See* ZUBOFF, *supra* note 72, at 128–32 (analyzing how tech platforms maintain continuous involvement throughout the data lifecycle).

[110] *See* Sheldon, *supra* note 14 (discussing the scope of data brokers' role).

[111] Kinza Yasar, *Web 2.0*, TECHTARGET (Jan. 30, 2023), https://www.techtarget.com/whatis/definition/Web-20-or-Web-2 [https://perma.cc/ZRH2-6UFV].

[112] *The History & Evolution of CRM: A Comprehensive Guide*, LOCALCRM (Sep. 9, 2022), https://localcrm.com/crm-the-history-evolution-of-crm/ [https://perma.cc/X4E4-7EQ8].

[113] *See id.*

[114] Nathan Sykes, *Mobile Apps and the Gamification of Data Collection*, TECHTALKS (June 20, 2019),

Although businesses assert these practices reflect a growing consumer demand for personalization, they also raise privacy concerns.[115] One frequently circulated example is that of Target sending targeted pregnancy ads to a pregnant teen based on her shopping history, effectively breaking the news to the girl's parents.[116] While shocking, this outlier horror story does not accurately reflect the way most companies employ data to offer consumers more tailored experiences.[117]

Despite valid concerns about data security and reselling first-party data, the privacy risks posed by individual businesses are notably less than those from Big Tech for two key reasons. First, competitive pressure incentivizes these businesses to respect privacy to maintain consumer trust.[118] Second, their relatively limited scale and scope of data collection limit individual risks compared to Big Tech's comprehensive surveillance capabilities.[119]

D. Current and Emerging Applications of Consumer Data

The full scope of consumer data usage remains unknown, as comprehensive proprietary protections shield many practices from public scrutiny, allowing companies to safeguard competitive advantages and avoid regulatory attention.[120] This Section examines both the documented applications of consumer data as well as emerging applications that raise novel privacy concerns.

1. Current Applications

Having designed their platforms to maximize consumer data capture and attention retention, Big Tech primarily monetizes this combination via targeted digital marketing.[121] For example, in 2023, targeted advertising

---

https://bdtechtalks.com/2019/06/20/mobile-app-game-data-collection-gamification/ [https://perma.cc/TL9W-HRQG].

[115] *See* Shep Hyken, *The Personalized Customer Experience: Customers Want You to Know Them*, FORBES (Apr. 17, 2024, at 11:52 ET), https://www.forbes.com/sites/shephyken/2024/04/14/the-personalized-customer-experience-customers-want-you-to-know-them/ [https://perma.cc/7X8G-PCYA].

[116] Henry Nunn, *Consumer Data Privacy and the First Amendment: The Right to Be Forgotten in a Room of Your Own*, 56 CREIGHTON L. REV. 541, 545 (2023).

[117] *See* Hyken, *supra* note 115.

[118] Jodi Daniels, *Consumer Trust Is Currency in the Digital Age: Here's How to Build It.*, FORBES (Aug. 8, 2023, at 09:45 ET), https://www.forbes.com/councils/forbesbusinesscouncil/2023/08/08/consumer-trust-is-currency-in-the-digital-age-heres-how-to-build-it/ [https://perma.cc/8DSX-G8HH].

[119] *See 4 Small Business Problems in Data Collection*, FORMASSEMBLY (May 1, 2023), https://www.formassembly.com/blog/small-business-data-collection-challenges/ [https://perma.cc/SPN7-NVWB].

[120] *See Companies Can Protect Proprietary Data When Responding to CCPA Privacy Requests*, GOODWIN (June 14, 2021), https://www.goodwinlaw.com/en/insights/publications/2021/06/06_14-companies-can-protect-proprietary-data [https://perma.cc/48FR-A6KX].

[121] Nathalie Maréchal & Ellery Roberts Biddle, *It's Not Just the Content, It's the Business Model: Democracy's Online Speech Challenge*, NEW AM. (Mar. 17, 2020),

generated 98 percent of Meta's $134 billion revenue,[122] 77 percent of Alphabet's $238 billion revenue,[123] and $49 billion for Amazon—a 24 percent annual increase.[124] Through sophisticated data analysis, these platforms combine demographic, psychographic, and behavioral data to deliver highly personalized advertisements.[125]

Beyond advertising, companies leverage consumer data for strategic decision-making, including decisions about product optimization and allocating internal human and financial capital.[126] Netflix analyzes both platform engagement and social media trends to inform content development,[127] while Amazon uses marketplace data to identify product opportunities—a practice that recently drew FTC scrutiny for potentially anti-competitive effects.[128] Platform personalization has become another crucial application, with algorithmic recommendations driving 35 percent of Amazon's sales and 75 percent of Netflix's views.[129] This practice has become so normalized that 75 percent of Americans now report being comfortable with personalized shopping recommendations.[130]

2. Emerging Applications

Due to the proprietary protections mentioned above, there is notably limited information available about many of the emerging applications of

---

https://www.newamerica.org/oti/reports/its-not-just-content-its-business-model/ [https://perma.cc/88LF-ZUT8].

[122] Matthew Johnston, *How Meta Generates Revenue Through Ads and the Metaverse,* INVESTOPEDIA (Oct. 10, 2025), https://www.investopedia.com/ask/answers/120114/how-does-facebook-fb-make-money.asp [https://perma.cc/T9VW-248A].

[123] *Annual Revenue of Alphabet from 2017 to 2024, by Segment*, STATISTA (Nov. 28, 2025), https://www.statista.com/statistics/633651/alphabet-annual-global-revenue-by-segment/ [https://perma.cc/2VZE-E5XA].

[124] Julia Faria, *Advertising Revenue of Amazon Worldwide from 2019-2024*, STATISTA (Nov. 29, 2025), https://www.statista.com/statistics/259814/amazons-worldwide-advertising-revenue-development/ [https://perma.cc/52QS-YLNX].

[125] *See Targeting*, RYTE, https://en.ryte.com/wiki/Targeting/ [https://perma.cc/BBA8-DAVT] (last visited Sep. 20, 2024).

[126] *See* Oleksii Svystun, *The Role of Data and Analytics in Proactive Product Improvement*, TECHSTACK (Aug. 22, 2024), https://tech-stack.com/blog/the-role-of-data-and-analytics-in-proactive-product-improvement/ [https://perma.cc/AQ29-C2MN].

[127] Thea Sokolowski, *How Data Drives Decision-Making at Netflix*, OUTSIDE INSIGHT, https://outsideinsight.com/insights/data-drives-decision-making-netflix/ [https://perma.cc/3NGD-5565] (last visited Sep. 20, 2024).

[128] *FTC Sues Amazon for Illegally Maintaining Monopoly Power*, FED. TRADE COMM'N (Sep. 26, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/09/ftc-sues-amazon-illegally-maintaining-monopoly-power [https://perma.cc/WLN6-ZC64].

[129] Ian MacKenzie, Chris Meyer & Steve Noble, *How Retailers Can Keep Up with Consumers,* MCKINSEY & CO. (Oct. 1, 2013), https://www.mckinsey.com/industries/retail/our-insights/how-retailers-can-keep-up-with-consumers [https://perma.cc/RJL5-MYS5].

[130] Mark Abraham, TR Geng, Florian Kogler & Lauren Taylor, *What Consumers Want from Personalization,* BOS. CONSULTING GRP. (Dec. 12, 2024), https://www.bcg.com/publications/2024/what-consumers-want-from-personalization [https://perma.cc/US5F-KAYL].

consumer data.[131] However, what is publicly known—including algorithmic behavioral modification, predictive health and behavior analysis, emotion recognition technology, and AI—is enough to raise novel privacy concerns.[132]

Algorithmic behavioral modification is something that all of Big Tech is known to employ to varying degrees.[133] In its pursuit to keep users scrolling, Meta's content algorithms are known to regularly push content optimized for emotions like outrage.[134] While Pokémon Go (released by Niantic, a Google start-up[135]) was so successful at influencing players' physical behavior, Niantic even had businesses paying to become Pokémon gyms to increase customer foot traffic.[136] Given a demonstrated propensity to employ these techniques and their proven profitability, Big Tech appears likely to continue developing sophisticated methods of influence.[137]

Predictive health analysis is an area many have speculated Big Tech could employ going forward[138] due to the influx of biometric health data captured via IoT devices such as phones, smartwatches, and other health trackers.[139] This data, when combined with unrelated and innocuous data points, such as search or location history, can reveal previously undetectable health insights.[140] For example, a 2020 study found changes in consumer behavior leading to a decline in credit score to be an accurate early predictor of dementia.[141] While there is certainly potential for beneficial innovation, such as earlier disease detection, the potential for exploiting these health insights for commercial gain raises serious privacy and ethical concerns.

Similarly, patent applications from numerous Big Tech companies—including Meta, Microsoft, and Alphabet—reveal a growing interest in

---

[131] *See* ZUBOFF, *supra* note 72, at 282–86 (discussing how tech companies maintain secrecy around their data practices through intellectual property protections and non-disclosure agreements).
[132] *See id.* at 293–96 (examining algorithmic behavior modification); *id.* at 247–52 (discussing predictive analytics); *id.* at 308–11 (analyzing emotion recognition technology); *id.* at 376–79 (addressing AI applications of collected data).
[133] *Id.* at 295–98 (documenting how major tech companies use behavioral modification algorithms).
[134] Matt M., *Everything You Need to Know About How Facebook Modifies Behavior and Why It Matters*, MEDIUM (Oct. 11, 2019), https://medium.com/@matt.flownotes/everything-you-need-to-know-about-how-facebook-modifies-behavior-and-why-it-matters-4223febf0f6f [https://perma.cc/Z35R-U6PR].
[135] *See* ZUBOFF, *supra* note 72, at 314.
[136] *See id.* at 316–17 (describing how Pokémon Go monetized "footfall" by having businesses pay to become game locations, demonstrating surveillance capitalism's ability to modify real-world behavior for profit).
[137] *See id.*
[138] *See* Kornelia Batko & Andrzej Ślęzak, *The Use of Big Data Analytics in Healthcare*, 9 J. BIG DATA 3, 3–10 (2022), [https://perma.cc/D678-3KCU] (discussing the potential uses of big data and new technology in healthcare).
[139] *See id.*
[140] *See id.*
[141] Kate Gibson, *Credit Score Decline Can Be an Early Warning for Dementia, Study Finds*, CBS NEWS (July 10, 2024, at 00:07 ET), https://www.cbsnews.com/news/credit-score-decline-may-be-early-warning-for-dementia-study-finds/ [https://perma.cc/HF42-BL4Y].

emotion recognition software.[142] This evolving technology analyzes various types of data to assess emotional states, examining biometric data from vocal tone and facial expressions during calls, as well as behavioral patterns like mouse movements and email tonality.[143] While not yet known to be deployed, this could foreseeably improve the efficacy of targeted advertising by enabling content delivery based on detected emotional states.

Perhaps most concerning are the emerging behavioral prediction capabilities of Big Tech. Attempting to predict future behavior is nothing new: Google has long understood the click probability of a search result based on its placement;[144] Amazon has similarly known about the increased probability of purchases based on when and how recommendations are presented.[145] However, increases in computing capacity and widespread availability of consumer data have transformed the degree to which Big Tech can accurately predict and subsequently sell these behavioral predictions.[146] Retired Harvard Business School Professor Shoshana Zuboff famously called these "behavioral futures markets," and they risk fundamentally reshaping the relationship between Big Tech and consumers as future behaviors are commodified and auctioned off to advertisers, all before a decision to act is ever made.[147]

Finally, AI represents the most transformative emerging application of consumer data, with Big Tech leveraging its vast repositories of consumer data to develop and train models in the race for AI supremacy.[148] This process requires a steady supply of clean, reliable data, something Big Tech has in mass.[149] Given this context, two key questions arise: Beyond the virtual agents and large language models commonly associated with contemporary AI, what unknown AI applications might Big Tech be developing?

---

[142] Nat Rubio-Licht, *Microsoft May Use Emotion Detection for "Richer" Work Meetings*, DAILY UPSIDE (Apr. 7, 2024), https://www.thedailyupside.com/technology/big-tech/microsoft-may-use-emotion-detection-for-richer-work-meetings/ [https://perma.cc/B7VF-HG66].

[143] Neil C. Hughes, *Emotion Tracking AI: A Tool for Empathy or Surveillance?*, CYBERNEWS (Feb. 12, 2025), https://cybernews.com/editorial/emotion-tracking-ai-empathy-surveillance/ [https://perma.cc/B38V-PHLC].

[144] Miranda Miller, *Click-Through Rate (CTR): Is It a Google Ranking Factor?*, SEARCH ENGINE J. (Oct. 17, 2021), https://www.searchenginejournal.com/ranking-factors/click-through-rate/ [https://perma.cc/Y5PP-2E2P].

[145] Larry Hardesty, *The History of Amazon's Recommendation Algorithm*, AMAZON SCI. (Nov. 22, 2019), https://www.amazon.science/the-history-of-amazons-recommendation-algorithm [https://perma.cc/37U3-MERF].

[146] *See* ZUBOFF, *supra* note 72, at 93–96 (explaining how increased computing power enables more accurate behavioral predictions).

[147] *Id.* at 96–97 (introducing the concept of "behavioral futures markets" where companies trade in predictions of future consumer behavior).

[148] THE POLYMATH PERSPECTIVE, *How Big Tech Is Secretly Using Your Data to Train AI: The Hidden Clauses in User Agreements*, MEDIUM (July 2, 2024), https://medium.com/@giant_chen1688/how-big-tech-is-secretly-using-your-data-to-train-ai-the-hidden-clauses-in-user-agreements-1173df47b64b [https://perma.cc/32XF-6MXJ].

[149] *See id.*

Moreover, with Big Tech companies collectively investing $150 billion annually in AI infrastructure,[150] necessitating an estimated $600 billion in new annual revenue to break even,[151] how will Big Tech monetize its AI assets going forward?

Part I has provided a foundational background of how consumer data is used throughout the modern digital economy, revealing two fundamental characteristics that complicate privacy regulation. First, the ability to collect and effectively utilize consumer data has become essential for business competition, creating market pressures that incentivize increasingly broad consumer surveillance. Second, Big Tech's dominance across markets, combined with its integrated platforms and vast data repositories, has given it unprecedented capabilities to accurately profile and predict consumer behavior. As AI emerges as a transformative technology, these capabilities and privacy concerns they raise seem likely to intensify. With this technical background established, Part II shifts focus to analyze the current regulatory landscape and its deficiencies in addressing these emerging challenges.

II. ANALYSIS OF THE CURRENT CONSUMER DATA PRIVACY LANDSCAPE

This Part provides a comprehensive analysis of consumer data privacy law and its fundamental issues. Starting first with an examination of the current regulatory framework—from the FTC's foundational role through the emergence of comprehensive state-level protections—the discussion analyzes how these various approaches have attempted to address privacy concerns. The analysis then examines three categories of systemic issues that plague these regulatory frameworks: the structural failures of Notice and Consent, challenges with enforcement and compliance, and significant gaps in secondary market oversight. Finally, this analysis concludes by exploring why proposed federal legislative solutions—while seemingly intuitive—remain impractical given the collective social, political, and market forces at play in the modern digital economy.

A. Current Regulatory Framework

This Section begins with an objective examination of current consumer data privacy laws that trace the evolution from early FTC enforcement to subject-specific laws, to the emergence of comprehensive privacy laws, and finally through recent failed attempts at passing federal legislation. To help

---

[150] Beth Kindig, *Big Tech Battles on AI, Here's the Winner*, FORBES (Aug. 8, 2024, at 21:24 ET), https://www.forbes.com/sites/bethkindig/2024/08/08/microsoft-leads-big-tech-in-ai-monetization-amazon-a-close-second/ [https://perma.cc/G3C3-RQHP].

[151] David Cahn, *AI's $600B Question*, SEQUOIA CAP. (June 20, 2024), https://www.sequoiacap.com/article/ais-600b-question/ [https://perma.cc/A39Q-CVXC].

make sense of the complex functionality of these laws, this review will focus on three key areas of these regulatory frameworks: the scope and limits, substantive rights granted to consumers, and enforcement mechanisms.

1. Evolution of FTC Privacy Enforcement

The FTC's role in privacy regulation traces back to its establishment under the Federal Trade Commission Act (FTCA) of 1914, which created the agency to prevent unfair methods of competition in commerce.[152] The Wheeler-Lea Act of 1938[153] expanded the FTC's Section 5 authority to include deceptive practices affecting commerce, [154] providing the foundation for its eventual role in privacy enforcement.[155]

By the 1980s, the FTC began applying this authority to emerging privacy concerns, initially focusing on telemarketing and credit reporting before shifting attention to internet privacy in the 1990s.[156] The 1998 GeoCities enforcement action marked a significant milestone, with the FTC using its Section 5 authority to address misrepresentation of website visitor data usage, resulting in mandatory privacy policy disclosures.[157] During this period, the FTC's approach to online privacy regulation evolved through two significant congressional reports.[158] The 1998 "Online Privacy" report criticized inadequate protections and established a regulatory framework that has evolved into today's Notice and Consent.[159] However, by 1999's "Self-Regulation and Privacy Online," the FTC had reversed course and endorsed industry self-regulation, explicitly recommending against legislative intervention.[160]

---

[152] Federal Trade Commission Act, Pub. L. No. 63-203, 38 Stat. 717 (1914) (codified as amended at 15 U.S.C. §§ 41-58 (2018)) [hereinafter FTCA].
[153] Wheeler-Lea Act of 1938, Pub. L. No. 75-447, 52 Stat. 111 (1938) (codified as amended at 15 U.S.C. § 45 (2018)).
[154] FTCA § 45(a)(1) ("Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful.").
[155] *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015) (affirming FTC's authority to regulate cybersecurity under Section 5).
[156] *See* Solove & Hartzog, *supra* note 30.
[157] Rachel Withers, *Before Facebook, There Was GeoCities*, SLATE (Apr. 16, 2018, at 08:07 ET), https://slate.com/technology/2018/04/the-ftcs-1998-case-against-geocities-laid-the-groundwork-for-facebook-debates-today.html [https://perma.cc/F7PL-L4MS].
[158] *See* FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998) [hereinafter PRIVACY ONLINE], https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf [https://perma.cc/NH5V-8YLW]; *see also* FED. TRADE COMM'N, SELF-REGULATION AND PRIVACY ONLINE: A REPORT TO CONGRESS 12–13 (1999) [hereinafter SELF-REGULATION], https://www.ftc.gov/system/files/documents/reports/self-regulation-privacy-onlinea-federal-trade-commission-report-congress/1999self-regulationreport.pdf [https://perma.cc/2MC7-LUPW].
[159] PRIVACY ONLINE, *supra* note 158, at 7.
[160] SELF-REGULATION, *supra* note 158, at 12–13.

While the FTC has become the country's de facto data protection authority, its regulatory power remains notably limited.[161] The agency lacks general rulemaking authority and cannot impose civil penalties on first-time violators.[162] Instead, it must rely on negotiated settlements with repeat offenders or pursue court-imposed penalties.[163] Additionally, the FTCA does not provide for a private right of action, leaving consumers without the ability to directly sue companies and reliant on FTC enforcement for unfair or deceptive practices.[164] Despite commissioners' repeated requests for expanded enforcement powers, Congress has not granted additional authority, leaving the FTC dependent on its "century-old Section 5 unfairness and deception authority."[165]

2. Subject Specific Data Privacy Legislation

In the absence of comprehensive federal privacy regulation, Congress has enacted several subject-specific privacy laws to address particularly sensitive categories of personal information. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 regulates the disclosure of identifiable health information,[166] including diagnoses, prescriptions, and associated demographic data.[167] Rather than granting specific patient rights, HIPAA imposes obligations on covered entities such as health plans, healthcare providers, and clearinghouses that electronically transmit health information.[168] The Department of Health and Human Services enforces HIPAA through civil penalties of up to $1.5 million annually,[169] while criminal violations can result in fines of up to $250,000 and imprisonment of up to 10 years.[170] Notably, HIPAA serves as a federal floor that allows states to impose more stringent protections.[171] It also does not create a private right

---

[161] *See* Solove & Hartzog, *supra* note 30, at 606.
[162] FED. TRADE COMM'N, FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY 7–8 (2020), https://www.ftc.gov/system/files/documents/reports/reports-response-senate-appropriations-committee-report-116-111-ftcs-use-its-authorities-resources/p065404reportprivacydatasecurity.pdf [https://perma.cc/2JNH-AW8Z].
[163] Rebecca Kelly Slaughter, Comm'r, Fed. Trade Comm'n, The Near Future of U.S. Privacy Law, Address at University of Colorado Law School 7 (Sep. 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf [https://perma.cc/E9JV-SUUA].
[164] Sean A. Pager & Eric Priest, *Redeeming Globalization Through Unfair Competition Law*, 41 CARDOZO L. REV. 2435, 2474 (2020).
[165] Slaughter, *supra* note 163, at 7.
[166] 45 C.F.R. § 160.103 (2023).
[167] Henry Nunn, *Consumer Data Privacy and the First Amendment: The Right to Be Forgotten in a Room of Your Own*, 56 CREIGHTON L. REV. 541, 545 (2023).
[168] 45 C.F.R. § 160.102 (2023).
[169] 42 U.S.C. § 1320d-5 (2018).
[170] *Id.* § 1320d-6.
[171] *Does the HIPAA Privacy Rule Preempt State Laws?*, U.S. DEP'T OF HEALTH & HUM. SERVS. (Dec. 28, 2022), https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html

of action, leaving enforcement exclusively to federal agencies.[172] Nor does it extend any protection to health information derived from the continued observation of consumers' online behavior.[173]

The Children's Online Privacy Protection Act (COPPA) of 1998 provides a more comprehensive regulatory framework for protecting children's online privacy.[174] The law requires operators of websites and online services to obtain verifiable parental consent before collecting personal information from children under 13, while also mandating clear notice about collection practices and data usage.[175] COPPA empowers parents with specific rights, including the ability to review collected data and demand its deletion.[176] The FTC enforces COPPA through civil penalties up to $51,744 per violation and can seek injunctive relief,[177] though the law notably lacks a private right of action.[178] Among online privacy laws, COPPA demonstrates how clear rights combined with stiff penalties can create effective deterrence, even within the Notice and Consent framework.[179]

Financial data privacy is primarily governed by three interconnected federal laws.[180] The Fair Credit Reporting Act (FCRA) of 1970 regulates consumer reporting agencies,[181] requiring them to ensure the accuracy of consumer information and granting consumers specific rights to access, dispute, and receive notice of adverse actions based on their credit reports.[182] The Fair and Accurate Credit Transactions Act (FACTA) expanded these protections in 2003,[183] adding requirements for data disposal and identity theft prevention while also strengthening enforcement mechanisms.[184] The Gramm-Leach-Bliley Act (GLBA) of 1999 complements this framework by

---

[https://perma.cc/Y2WX-F26D].

[172] *See* Dodd v. Jones, 623 F.3d 563, 569 (8th Cir. 2010) (finding that a plaintiff's claim failed because "HIPAA does not provide a private right of action").

[173] Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y L. & ETHICS 143, 194 (2017) (discussing HIPAA's limitations regarding non-covered entities and modern health data collection).

[174] *See* 15 U.S.C. §§ 6501-6506 (2018).

[175] *Id.* § 6502(b)(1)(A).

[176] *Id.* § 6502(b)(1)(B).

[177] *Complying with COPPA: Frequently Asked Questions*, FED. TRADE COMM'N (Jan. 2025), https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions [https://perma.cc/9S5P-66UP].

[178] Miles Light, *Think of the Children: A Comparison of APRA and COPPA 2.0*, BBB NAT'L PROGRAMS (May 6, 2024), https://bbbprograms.org/media-center/bd/insights/2024/05/06/comparison-apra-coppa-2.0 [https://perma.cc/HQ7Y-JTYL].

[179] *See id.*

[180] *See* Dori K. Bailey, Savanna P. Klinek & Shannon A. Knapp, *Financial Data Privacy: CFPB Updates*, BOND SCHOENECK & KING ATTORNEYS (Jan. 23, 2025), https://www.bsk.com/news-events-videos/financial-data-privacy-cfpb-updates [https://perma.cc/FDC8-ZHDW].

[181] 15 U.S.C. § 1681s.

[182] *Id.* §§ 1681i, 1681j, 1681m(a).

[183] *Id.* §§ 1681-1681x.

[184] *Id.* §§ 1681m(e)(1)(A), 1681w(1), 1681s.

imposing affirmative duties on financial institutions to protect consumers' nonpublic information,[185] requiring consumer notification before third-party disclosure, and enabling opt-out rights for data sharing.[186]

Enforcement authority for these financial data privacy laws is divided among federal agencies and state Attorneys General, with the FTC and Consumer Financial Protection Bureau primarily empowered to impose civil penalties ranging from $2,500 to $100,000 per violation[187] and criminal penalties under GLBA of up to 5 years in prison.[188] While the FACTA expanded FCRA provides consumers with a private right of action for willful or negligent noncompliance,[189] GLBA relies solely on agency enforcement.[190] This multi-agency structure, while leveraging existing regulatory expertise, has led to criticism about inconsistent application and enforcement gaps.[191]

Most recently, some states have begun addressing biometric data privacy through targeted legislation. Illinois's Biometric Information Privacy Act (BIPA), enacted in 2008, established the first comprehensive framework for protecting biometric data—including fingerprints, facial scans, and other unique biological characteristics.[192] BIPA requires private entities to obtain written consent before collecting biometric data, maintain publicly available data retention policies, and refrain from selling or profiting from collected information.[193] In addition to allocating enforcement authority to the Attorney General's Office,[194] BIPA provides individuals with a private right of action, enabling statutory damages up to $5,000 per intentional or reckless violation.[195]

Texas followed suit by passing the Capture or Use of Biometric Identifier Act (CUBI) in 2009, which shares similar protections as BIPA but embraces a different approach to enforcement.[196] While CUBI also requires informed

---

[185] *Id.* § 6801(a).
[186] *Id.* § 6802(a)–(b).
[187] Katy Liu, *Guide to the Gramm-Leach-Bliley Act*, IAPP (Feb. 24, 2018), https://iapp.org/resources/article/guide-to-the-gramm-leach-bliley-act/ [https://perma.cc/3J2A-FXF6]; *see* 15 U.S.C. § 1681s.
[188] 15 U.S.C. § 6823(a).
[189] *Id.* § 1681s.
[190] *See* NAT'L ASS'N OF INS. COMM'RS, GLBA & HIPAA PRIV. COMPARISON CHART 11 (2020), https://content.naic.org/sites/default/files/inline-files/GLBA%20HIPAA%20%20Privacy%20Comparison%20Chart_0.pdf [https://perma.cc/6E2W-NGKU] (showing how GLBA does not create a private right of action).
[191] *See* Edward J. Janger & Paul M. Schwartz, *The Gramm-Leach-Bliley Act, Information Privacy, and the Limits of Default Rules*, 86 MINN. L. REV. 1219, 1230-32 (2002).
[192] *Is Biometric Information Protected by Privacy Laws?*, BL (June 20, 2024), https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/ [https://perma.cc/6WRF-WMMC].
[193] *Id.*
[194] 740 ILL. COMP. STAT. ANN. 14/25 (2008).
[195] *Id.* 14/20 (2008).
[196] TEX. BUS. & COM. CODE § 503.001 (West 2009).

consent for biometric data collection and mandates timely data destruction,[197] it relies solely on the state Attorney General for enforcement through civil penalties of up to $25,000 per violation, and does not permit a private right of action.[198]

Both BIPA and CUBI have led to historic settlements with Big Tech firms that disregarded these regulations. In 2020, BIPA led to a then-historic $650 million class-action settlement in *Patel v. Facebook*, where a class of Facebook users accused Facebook of illegally collecting and keeping their biometric information.[199] Not to be outdone, in 2024, CUBI led to the Texas Attorney General successfully securing a $1.4 billion settlement from Meta, followed by a $1.375 billion settlement with Google in 2025, which are the largest settlements ever obtained by a single state to date.[200] These settlements demonstrate how subject-specific state privacy laws, especially when backed by substantial penalties and diverse enforcement mechanisms, can create effective deterrence while financially incentivizing other states to adopt similar protections.[201]

3. Comprehensive Privacy Frameworks

The recent emergence of comprehensive privacy frameworks represents a shifting approach to regulating data, moving beyond the limited scope of subject-specific laws to establish broader protections for consumer data. Starting with GDPR's implementation of the first truly comprehensive framework with global reach, followed by California's influential California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA), and a subsequent influx of copycat state laws, these laws share the common framework of combining business obligations with foundational consumer rights.[202] However, significant variations in scope, requirements, and

---

[197] *Id.* §§ 503.001(b), (c)(3).
[198] *Id.* § 503.001(d).
[199] *Is Biometric Information Protected by Privacy Laws?*, *supra* note 192.
[200] Press Release from Office of Attorney General of Texas Attorney General Ken Paxton, Secures $1.4 Billion Settlement with Meta Over Its Unauthorized Capture of Personal Biometric Data in Largest Settlement Ever Obtained from an Action Brought by a Single State (July 30, 2024), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-14-billion-settlement-meta-over-its-unauthorized-capture [https://perma.cc/28QU-3NFK]; Press Release from Office of Attorney General of Texas Attorney General Ken Paxton, Attorney General Ken Paxton Secures Historic $1.375 Billion Settlement with Google Related to Texans' Data Privacy Rights (May 9, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-secures-historic-1375-billion-settlement-google-related-texans-data [https://perma.cc/ T75F-JA9N].
[201] *See Is Biometric Information Protected by Privacy Laws?*, *supra* note 192.
[202] *See Preparing for 2025: A Dive into New U.S. Data Privacy Laws*, TRUSTARC, https://trustarc.com/resource/preparing-2025-new-data-privacy-laws/ [https://perma.cc/GC54-6GM8] (last visited Feb. 5, 2025).

enforcement mechanisms across jurisdictions have created a complex regulatory landscape for businesses seeking to comply.[203]

i. The GDPR Model

The European Union's GDPR, implemented in 2018, established a comprehensive framework for data privacy protection, representing a watershed moment as the first data privacy regulation with global reach.[204] Rather than targeting specific types of data or business sectors, GDPR's framework creates a uniform privacy standard across all EU member states[205] by placing obligations on businesses that possess and process consumer data and provides consumers with explicit data privacy rights.[206]

The scope of GDPR extends beyond traditional territorial boundaries, applying to any entity that processes the personal data of EU residents, regardless of the company's location.[207] In effect, this has forced businesses worldwide to reassess their data handling procedures or risk heavy fines.[208] GDPR regulates businesses through a dual framework of controllers and processors.[209] Controllers, who determine the purposes and methods of data processing, are responsible for ensuring both their own and their processor's activities comply with GDPR and for implementing adequate security measures.[210] Processors, who handle data on behalf of controllers, must follow strict processing guidelines, maintain detailed records, and report directly to controllers.[211] Both entities must designate Data Protection Officers, report breaches within 72 hours, and document all processing activities.[212] Failure to maintain adequate security measures or properly report breaches can result in fines of up to €10 million or two percent of global revenue.[213]

Additionally, GDPR provides consumers with a comprehensive set of eight fundamental privacy rights, empowering individuals with more control over their personal data.[214] These rights include the right to: be informed about the collection and use of personal data; access and obtain collected

---

[203] *See id.*
[204] General Data Protection Regulation, art. 46, 2016 O.J. (L 119) 1 [hereinafter GDPR].
[205] Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 122–23 (2017).
[206] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 99–100 (2021).
[207] GDPR, art. 3(2).
[208] Paul M. Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 784 (2019).
[209] GDPR, art. 4(7).
[210] *Id.* arts. 5(1), 24.
[211] *Id.* art. 28.
[212] *Id.* arts. 37, 33, 30.
[213] *Id.* art. 83.
[214] *Id.* arts. 13–22.

data; rectify inaccurate or incomplete data; erase data; restrict or object to data processing; and opt out of automated decision-making and profiling using their personal data.[215] While these rights contain various qualifications and exceptions that chip away at their comprehensiveness, this list represents an important and novel legal framework for consumer privacy regulation.[216]

Enforcement authority is primarily delegated to national supervisory authorities,[217] which are empowered to investigate complaints, conduct audits, and impose substantial penalties.[218] For serious violations, GDPR employs a tiered penalty structure with fines of up to €20 million or four percent of gross annual revenue, whichever is higher.[219] This enforcement framework has proven notably effective, as demonstrated by recent penalties for unauthorized data processing, including Meta's €1.2 billion fine in 2023 and Amazon's €746 million fine in 2021.[220]

This combination of a broad scope framework to regulate business and comprehensive consumer privacy rights, coupled with robust enforcement mechanisms and stiff penalties for noncompliance, has made GDPR the de facto global standard for consumer data privacy.[221] GDPR's impact has been particularly significant in the United States (U.S.), where businesses with international footprints have been forced to adopt GDPR-compliant practices or risk hefty fines.[222] Moreover, GDPR has served as the global blueprint for subsequent data protection laws, including California's CCPA.[223]

ii. State-Level Implementation: CCPA and Beyond

The CCPA, effective in 2020 and subsequently amended by the California Privacy Rights Act (CPRA) in 2023, established the United States' first comprehensive data privacy framework.[224] Passed in response to growing concerns over data breaches, the monetization of personal data, and the Cambridge Analytica scandal, the CCPA set a de facto national standard for

---

[215] *Id.*
[216] *See A Guide to the Data Protection Exemptions*, INFO. COMM'R'S OFF. (Sep. 29, 2022), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/exemptions/a-guide-to-the-data-protection-exemptions/ [https://perma.cc/23LE-XWX3] (detailing the various exceptions and limitations to GDPR rights while noting how the overall framework remains a groundbreaking approach to privacy protection).
[217] GDPR, art. 51.
[218] *Id.* art. 58.
[219] *Id.* art. 83(5).
[220] *20 Biggest GDPR Fines So Far [2025]*, DATA PRIV. MANAGER (Mar. 3, 2025), https://dataprivacymanager.net/5-biggest-gdpr-fines-so-far-2020/ [https://perma.cc/3NXQ-S7AT].
[221] Schwartz, *supra* note 208, at 772.
[222] *See id.* at 805.
[223] *See id.* at 817.
[224] Taylor M. Lammonds, *Consumer Data Privacy: A Federal Standard May Be the Cure for Business Compliance*, 45 CAMPBELL L. REV. 109, 115–16 (2022).

consumer data privacy.[225] Modeled after the GDPR framework, these laws both regulate the data privacy practices of businesses and grant California residents a foundational set of privacy rights.[226] However, unlike GDPR's universal application, CCPA applies only to for-profit businesses that operate in California and meet specific thresholds: annual revenues exceed $25 million; process personal data of over 100,000 consumers or households; or derive over half their annual revenue from selling consumer data.[227]

The regulatory framework imposes specific obligations on covered businesses.[228] Companies must provide clear notice before collecting data, including categories of data collected and intended uses.[229] The law restricts data collection to what is "reasonably necessary" for disclosed purposes, requires explicit retention policies, mandates "reasonable" security measures, and necessitates contractual protections for third-party data transfers.[230] Businesses must also establish processes by which consumers can exercise their rights, including that businesses respond to requests within 45 days.[231]

In addition to this regulatory framework imposed on businesses, CPRA expanded CCPA's original consumer rights framework to include: knowledge of what personal information is collected and shared; deletion of personal information; correction of inaccurate data; opt-out rights for data sales and sharing; and limitations on sensitive data use.[232] While these rights largely mirror the GDPR's framework, their implementation is more limited in scope, particularly because of the CPRA's narrower applicability to certain businesses and its state-level enforcement, as well as more specific exemptions for data retention and fewer provisions for children's data and data portability.[233]

Enforcement authority initially rested solely with California's Attorney General[234] but expanded under CPRA with the creation of the California Privacy Protection Agency (CPPA).[235] Both entities can impose civil penalties up to $2,500 per violation, increased to $7,500 for intentional

---

[225] Schwartz, *supra* note 208, at 816.
[226] Lammonds, *supra* note 224, at 114.
[227] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.140(d). (West 2023) [hereinafter CCPA].
[228] *Id.* § 1798.100.
[229] *Id.* § 1798.100(a).
[230] *Id.* §§ 1798.100(c), (a)(3), (d), (e).
[231] *Id.* § 1798.130(a).
[232] *Id.* §§ 1798.110, 1798.105, 1798.106, 1798.121.
[233] *Compare* CCPA §§ 1798.100(a)–(d), 1798.140(c)(1) (limiting application to businesses meeting specific thresholds and providing a narrower rights framework), *with* GDPR, arts. 8, 15–20 (establishing a broader rights framework, including enhanced protections for children's data and comprehensive data portability provisions).
[234] Lammonds, *supra* note 224, at 116.
[235] CCPA § 1798.199.10.

violations or those involving minors.[236] The law provides a limited private right of action for data breaches resulting from inadequate security measures,[237] with statutory damages of $100 to $750 per consumer per incident, or actual damages, whichever is greater.[238] Compared to GDPR's comprehensive security requirements, CCPA takes a more limited approach to data breaches, requiring businesses to implement "reasonable security procedures."[239]

Unlike GDPR's revenue-based penalties, these fixed amounts have produced less impactful enforcement outcomes.[240] For example, in September 2022, Sephora settled for $1.2 million for failing to honor opt-out requests.[241] More recently**,** in June 2024**,** California Attorney General Bonta announced the largest penalty ever levied under CCPA, a historic $1.55 million settlement with Healthline Media LLC for sharing consumers' sensitive health-related tracking information without proper opt-out options.[242] Considering these relatively modest amounts, it is reasonable to question the practical deterrent effect of CCPA, as $1.2 million is unlikely to dissuade Big Tech firms with market capitalizations in excess of $1 trillion. Still, CCPA should be appreciated for what it is, the first comprehensive consumer data privacy law in the country, which has set forth a model legal framework that many subsequent state laws copied.[243]

iii. The Emerging Patchwork Problem

Following California's lead, 20 states have enacted comprehensive privacy laws as of April 2025, with several more whose proposed Bills are working their way through state legislatures.[244] Due to how recently most of these laws were enacted, with many yet to take effect, there is a limited

---

[236] *Id.* § 1798.199.90.
[237] *Id.* § 1798.150.
[238] *Id.*
[239] *Compare* GDPR arts. 32, 25, *with* CCPA § 1798.150(a)(1) (imposing liability standard based on reasonableness rather than specific measures).
[240] *See GDPR vs. CCPA: A Thorough Breakdown of Data Protection Laws*, THOROPASS: BLOG, https://thoropass.com/blog/compliance/gdpr-vs-ccpa/ [https://perma.cc/5A68-VG6T] (last visited Feb. 5, 2025).
[241] Press Release from California Attorney General Rob Bonta, Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act (Aug. 24, 2022), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement [https://perma.cc/3DNZ-9TDL].
[242] Press Release from California Attorney General Rob Bonta, Attorney General Bonta Announces Largest CCPA Settlement to Date, Secures $1.55 Million from Healthline.com (July 1, 2025), https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-largest-ccpa-settlement-date-secures-155 [https://perma.cc/ 9SJA-BTW6].
[243] Lammonds, *supra* note 224, at 112.
[244] *Which States Have Consumer Data Privacy Laws?*, BL (Apr. 7, 2025), https://pro.bloomberglaw.com/insights/privacy/state-privacy-legislation-tracker/ [https://perma.cc/3CRK-7BFM].

sample size to interpret from.[245] While these laws generally follow the same GDPR/CCPA framework that combines business regulations with foundational consumer privacy rights, significant variations exist in their scope, obligations, and enforcement mechanisms, creating a complex regulatory landscape for interstate commerce.[246]

Virginia's Consumer Data Protection Act (VCDPA), implemented in 2023, and Colorado's Privacy Act (CPA) in 2024, best illustrate these variations.[247] On the business regulation side, both laws avoid CCPA's revenue threshold, focusing instead on data processing volume.[248] VCDPA applies to businesses that process data from 100,000 consumers or derive significant revenue from data sales, while CPA sets a lower threshold of 25,000 consumers for data sale provisions.[249] Both grant core privacy rights—access, deletion, correction, and opt-out rights for targeted advertising,[250] but are less comprehensive than the CCPA's consumer rights. Enforcement mechanisms are also more limited, with neither providing private rights of action, instead relying on state agencies.[251] However, Colorado does authorize penalties up to $20,000 per violation,[252] which is notably above what California and Virginia allow at $7,500.[253] There are currently no publicly reported enforcement actions or significant settlements due to how recently these laws were passed, as well as the time required to investigate violations and bring a case.

State data privacy regulations also differ significantly in how they define and treat various types of data. While regulating personal information serves as the foundational principle of these laws, the exact definition varies across jurisdictions. Utah's Consumer Privacy Act adopts a narrower approach, enumerating specific categories of protected information such as real names, identification numbers, and precise geolocation data.[254] In contrast, California and Connecticut take a more expansive approach, protecting not just enumerated categories but any information reasonably capable of being linked to consumers or households.[255] Treatment of sensitive data categories also varies between state regulations. For example, Virginia requires explicit opt-in consent before processing sensitive data that includes precise

---

[245] *See id.*
[246] *See* Suzanne Bernstein, *Consumer Data Protection and Privacy: A Proposal for a New Law and an Independent Agency*, 83 U. PITT. L. REV. ONLINE 1, 18 (2022).
[247] *See Which States Have Consumer Data Privacy Laws?*, *supra* note 244.
[248] COLO. REV. STAT. § 6-1-1304(1) (2021); VA. CODE ANN. § 59.1-576(A) (2021).
[249] COLO. REV. STAT. § 6-1-1304(1); VA. CODE ANN. § 59.1-576(A).
[250] COLO. REV. STAT. § 6-1-1306(1); VA. CODE ANN. § 59.1-577.
[251] COLO. REV. STAT. § 6-1-1311; VA. CODE ANN. § 59.1-584.
[252] COLO. REV. STAT. § 6-1-112(1)(a).
[253] CCPA § 1798.199.90; VA. CODE ANN. § 59.1-584.
[254] UTAH CODE ANN. § 13-61-101(23) (2023).
[255] CONN. GEN. STAT. § 42-516(18) (2023); CCPA § 1798.140(v)(1).

geolocation, genetic data, or biometric information.[256] Comparatively, Nevada treats all covered data uniformly, applying the same level of protection to sensitive biometric data as it does to basic contact information.[257] These differences highlight the regulatory inconsistencies that exist across jurisdictions.

Approaches to data security and breach notification requirements also vary significantly. While all 50 states have breach notification laws, requirements for what constitutes "reasonable" security measures differ substantially.[258] Some states, like New York, require specific technical safeguards,[259] while others provide only general guidance, creating additional compliance challenges for businesses.[260]

This patchwork approach of state laws has attracted criticism from both sides. Privacy advocates point out systemic flaws due to the reliance on resource-constrained state agencies and the lack of a private right to action.[261] On the other hand, business advocates criticize the patchwork regulatory approach, which creates compliance challenges because regulations vary across jurisdictions.[262] Despite these criticisms, the state-level approach has produced two notable benefits: the increased probability of business compliance through the expanded oversight and extension of basic privacy protections beyond California.[263] Still, the inherent issues of this fragmented system have led many to conclude that a superseding federal data privacy law is needed.

4. Failed Federal Legislative Attempts

Despite strong bipartisan public support,[264] the U.S. still lacks any comprehensive federal privacy legislation, due in part to extreme partisanship and effective industry lobbying by Big Tech.[265] Early attempts

---

[256] VA. CODE ANN. §§ 59.1-578(A)(5), 59.1-575.
[257] NEV. REV. STAT. §§ 603A.310, 603A.320, 603A.330 (2021).
[258] *See Security Breach Notification Laws*, NCSL (Jan. 17, 2022), https://www.ncsl.org/technology-and-communication/security-breach-notification-laws [https://perma.cc/2JZZ-U26R].
[259] N.Y. COMP. CODES R. & REGS. tit. 23, § 500 (2023).
[260] *See* David Thaw, *The Efficacy of Cybersecurity Regulation*, 30 GA. ST. U. L. REV. 287, 326 (2014) (analyzing how inconsistent definitions of "reasonable" security measures across state regulations create compliance challenges for businesses).
[261] Keely Quinlan, *State Privacy Laws Largely Fail to Protect Consumer Data, Report Shows*, STATESCOOP (Feb. 2, 2024), https://statescoop.com/state-privacy-laws-fail-protect-consumer-data-2024/ [https://perma.cc/T9PB-53J9].
[262] Bernstein, *supra* note 246, at 12.
[263] *See id.* at 31.
[264] Colleen McClain et al., *How Americans View Data Privacy*, PEW RSCH. CTR. (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/ [https://perma.cc/73R6-AYW8].
[265] Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES: WIRECUTTER (Sep. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-

included the Consumer Online Privacy Rights Act (COPRA), introduced by Senate Democrats in 2019, which proposed a GDPR-style framework with broad consumer rights and a private right of action.[266] Senate Republicans countered with the SAFE DATA Act in 2020, which maintained a similar framework as COPRA but relied solely on FTC and state enforcement, lacked a private right of action, and preempted state privacy laws in an effort to address the effects of patchwork regulation.[267] Both Bills failed to advance beyond committee, showcasing the partisan divide over enforcement mechanisms and state law preemption.[268]

Following these failed attempts, in 2022, a bipartisan group of Congresspeople supported by several Senators introduced the American Data Privacy and Protection Act (ADPPA).[269] The Bill's proposed regulatory framework generally followed the GDPR structure: applying to covered entities that collect, process, or transfer data and providing consumers with a broad set of foundational privacy rights—including access, deletion, correction, and portability.[270] ADPPA also included novel provisions tailored to address emerging data privacy challenges, such as data minimization, algorithmic impact assessments, and enhanced protections for sensitive data categories.[271] Its enforcement framework allocated broad authority to the FTC and state Attorneys General while permitting a notably limited private right of action and preempting most state privacy laws.[272] ADPPA advanced further than previous attempts, making it out of committee and onto the House floor.[273] However, because of significant lobbying by Big Tech, partisan concerns over preemption of state laws, and criticism of the Bill's weak enforcement mechanisms from Senate Commerce Chair Cantwell, ADPPA never made it to a vote on the House floor.[274]

Most recently, in 2024, the American Privacy Rights Act (APRA) was introduced by a bipartisan and bicameral group of lawmakers, including Senator Cantwell.[275] The Bill maintained the same general structure as

---

us/ [https://perma.cc/Q7FZ-CGMT].
[266] *See* S. 2968, 116th Cong. §§ 101–106, 301 (2019).
[267] *See* S. 4626, 116th Cong. §§ 401–402, 405 (2020).
[268] Ash Johnson, *Three Bills Show Remaining Divisions in Attempt to Reach a Compromise on Federal Data Privacy Legislation*, INFO. TECH. & INNOVATION FOUND. (June 17, 2022), https://itif.org/publications/2022/06/17/bills-show-remaining-divisions-on-federal-data-privacy-legislation/ [https://perma.cc/3LTL-ZETT].
[269] H.R. 8152, 117th Cong. (2022).
[270] *See id.* §§ 2(9), 102, 103.
[271] *See id.* §§ 101, 207, 208.
[272] *See id*. §§ 401–404.
[273] *See* Margaret Harding McGill, *Online Privacy Bill Faces Daunting Roadblocks*, AXIOS (Aug. 4, 2022), https://www.axios.com/2022/08/04/online-privacy-bill-roadblocks-congress [https://perma.cc/D3N5-XX62].
[274] *See id.*
[275] *See* H.R. 8818, 118th Cong. (2024).

preceding Bills,[276] while introducing several key differences, including the complete exemption of small businesses (defined by revenue or employee thresholds), a more expansive preemption of state law than ADPPA, and the creation of a new Bureau of Privacy within the FTC to carry out enforcement.[277] After revisions to the Bill that commentators characterized as "engineered to appease conservative lobbyists representing the interests of big business," APRA became a Bill that satiated the goals of neither privacy advocates nor industry stakeholders, leading House Republican leadership to effectively kill the Bill.[278]

Collectively, this analysis of the current legal landscape highlights the challenges in crafting and enacting legislation that successfully balances consumer protection with competing business interests. While some progress has been made through subject-specific legislation and the emerging patchwork of comprehensive state laws, data privacy laws remain fragmented and inconsistent.[279] The FTC continues to operate with limited authority, state laws vary significantly in key requirements and enforcement mechanisms, and efforts to establish comprehensive federal legislation have repeatedly failed despite broad public support.[280] The following Section further explores these shortcomings through some of the most prolific critiques of the current regulatory landscape.

B. Fundamental Issues with Current Privacy Regulation

Beyond the previously discussed limitations of individual privacy laws, the collective legal landscape suffers from three systemic issues that fundamentally undermine regulatory efficacy. First, the Notice and Consent model has proven fundamentally defective as a legal framework, providing neither meaningful notice nor genuine consent for data collection.[281] Second, the multi-state regulatory patchwork creates numerous enforcement and compliance challenges that render it impotent at addressing business concerns or protecting consumer privacy.[282] Lastly, substantial regulatory gaps throughout the secondary market enable the unrestricted flow of consumer data far beyond the consent scope of initial collection, nullifying

---

[276] *See id.* §§ 2(21), 101–104.
[277] *See id.* §§ 2(20), 201, 404.
[278] Dell Cameron, *Surprise! The Latest 'Comprehensive' US Privacy Bill Is Doomed*, WIRED (June 27, 2024, at 11:55 ET), https://www.wired.com/story/apra-privacy-bill-doomed/ [https://perma.cc/85QC-98TR].
[279] *See States Rights and US Data Privacy Fragmentation*, COOKIEHUB https://www.cookiehub.com/blog/states-rights-and-us-data-privacy-fragmentation [https://perma.cc/2MA3-E9MW] (last visited Nov. 16, 2025).
[280] *See* Cameron, *supra* note 278.
[281] *See* discussion *infra* Section II.B.1.
[282] *See* discussion *infra* Section II.B.2.

any pretense of consumer control over their personal information.[283] Taken together, these critiques expose systemic weaknesses that plague the current approach to regulating consumer data.

1. The Structural Failures of Notice and Consent

The Notice and Consent legal framework provides, at least in theory, that consumer data collection is legally permissible so long as consumers are provided adequate notice of and consent to businesses' terms.[284] Proponents argue this framework is built upon a mutually bargained-for exchange where consumers are generally aware of this process and trade personal data for free services.[285] However, the inherent irony of this framework is that consumers deprived of adequate notice are unable to meaningfully consent to terms they do not understand, rendering this framework substantively deficient.[286]

This is by design, a feature of the system rather than a bug. These agreements are intentionally written in complex legalese, incomprehensible to non-lawyers, and at lengths that effectively discourage consumers from even attempting to read them.[287] For example, one study found that a majority of participants ignored the terms altogether, with 81 percent of the remaining participants spending less than one minute reading the terms.[288] Critics point out that consumers were never the intended audience for these agreements; rather, "[i]n-house counsel know that the only real audiences for the platform terms are the FTC, judges, and plaintiff's counsel, and they draft accordingly."[289] Moreover, the current marketplace offers no meaningful privacy-protective alternatives.[290] For example, DuckDuckGo is the most prominent privacy-focused browser and search engine, yet it has only captured a 0.78 percent market share.[291]

---

[283] *See* discussion *infra* Section II.B.3.

[284] Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, NEW AM.: BLOG (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/ [https://perma.cc/Y8JU-F9VB].

[285] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 105 (2010) (analyzing the common arguments made by proponents in support of consumers' ability to exchange personal data for services).

[286] Thomas D. Haley*, Illusory Privacy*, 98 IND. L.J. 75, 116 (2022).

[287] *See id.* at 93.

[288] *Id.* at 88 (citing Jonathan A. Obar & Anne Oeldorf-Hirsch, *The Biggest Lie on the Internet: Ignoring the Privacy Policies and Terms of Service Policies of Social Networking Services*, 23 INFO., COMMC'N & SOC'Y 1, 12, 16 (2018)).

[289] *Id.* at 117 (alteration in original).

[290] *Id.* at 101.

[291] *Search Engine Market Share Worldwide - January 2026,* STATCOUNTER GLOBALSTATS, https://gs.statcounter.com/search-engine-market-share [https://perma.cc/FC2A-JVVT]. (last visited Jan. 7, 2026).

Consistent with notice mechanisms are equally deficient consent mechanisms. Commonly presented as clickwrap or browsewrap agreements that simply require a consumer to either click "I agree" or continue browsing a website,[292] these agreements are designed to make the minimal legally required effort to obtain consent while being strategically placed along the consumer journey to maximize the probability of assent.[293]

While the deficiencies of clickwrap and browsewrap agreements as consent capture mechanisms are well documented, alternative approaches such as Express Consent mandated by the GDPR have proven equally problematic.[294] Express Consent requires consumers to voluntarily and affirmatively provide consent to data collection every time.[295] This inevitably leads to a phenomenon called consent fatigue, where inundated consumers who have grown apathetic to requests click accept, ultimately resulting in a lack of meaningful consent.[296] Despite these flaws, Notice and Consent remains foundational to American data privacy law, with even the generally praised CCPA relying upon this troublesome framework.[297]

The most damning criticism of the Notice and Consent framework concerns three specific rights that businesses regularly insert into their privacy agreements: the right to unilaterally modify platform terms, the right to change service offerings, and the right to transfer consumer data in the event of a merger or sale.[298] If businesses retain the right to unilaterally modify the terms of the agreement, it "renders the choice to skip reading terms and conditions not only rational but inevitable."[299] This concern extends to the service offerings clause, which Meta famously exercised in 2024 when repurposing historical user data to train its AI models:[300] a use case beyond the foreseeable scope of what consumers agreed to when initially accepting its privacy policy. The same can be said for the merger or sale clause, which came up when Google acquired Fitbit, absorbing all its

---

[292] Haley, *supra* note 286, at 82.
[293] *See* Neel Chatterjee & Victor Wang, *Best Practices for Designing Clickwrap Agreements*, DOCUSIGN (July 20, 2020), https://www.docusign.com/blog/best-practices-designing-clickwrap-agreements [https://perma.cc/QQ2Z-TS75].
[294] Daniel J. Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. 593, 597 (2024).
[295] *Id.*
[296] *Id.*
[297] Haley, *supra* note 286, at 93.
[298] *Id.* at 100.
[299] *Id.* at 103.
[300] *Meta Is Using Your Photos to Train Its AI: Here's What You Need to Know*, BLOCK PARTY (Aug. 1, 2024), https://www.blockpartyapp.com/blog/meta-is-using-your-photos-to-train-its-ai-heres-what-you-need-to-know/ [https://perma.cc/QCB3-62F3].

consumer biometric health data, while not being contractually bound by the Fitbit privacy policy consumers had agreed to.[301]

Collectively, these three reserved rights render Notice and Consent defective as a legal framework, whose terms become meaningless and devoid of consent when they can be unilaterally changed after the fact. Consequently, no reasonable person—including the Chief Justice of the Supreme Court—would waste time reading such fine print.[302]

2. Enforcement and Compliance Challenges

The effectiveness of privacy regulations is also undermined by enforcement and compliance challenges that contribute to systemic inefficiencies.[303] Individual state-level enforcement mechanisms suffer from both resource constraints and inadequate deterrence frameworks.[304] While businesses face confusing and burdensome compliance requirements across multiple regulatory schemas, they are forced to navigate.[305]

Most state privacy laws primarily task their Attorney General offices with enforcement, which in practice proves challenging.[306] These state agencies were already budget and staffing-constrained, unable to meet existing obligations prior to the passage of data privacy laws.[307] Given the technical complexity and opaque nature of modern data practices, the resources needed to detect violations, gather evidence, and successfully litigate against well-resourced businesses are beyond what many state agencies have to spend.[308] While states could allow for a private right of action to help supplement these resource-constrained state agencies, the vast majority of state laws do not.[309] Leaving the public options to fall short of what many would consider effective enforcement.

---

[301] Haley, *supra* note 286, at 113–14.

[302] Debra Cassens Weiss, *Chief Justice Roberts Admits He Doesn't Read the Computer Fine Print*, A.B.A. J. (Oct. 20, 2010, at 12:17 CT), https://www.abajournal.com/news/article/chief_justice_roberts_admits_he_doesnt_read_the_computer_fine_print [https://perma.cc/X2KU-K9PL].

[303] *See* Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 S. CAL. L. REV. 1529, 1567–69 (2019) (examining broader systemic failures in privacy law enforcement and compliance mechanisms).

[304] *See id.*

[305] *See id.*

[306] *See* CAITRIONA FITZGERALD, KARA WILLIAMS & R.J. CROSS, THE STATE OF PRIVACY: HOW STATE "PRIVACY" LAWS FAIL TO PROTECT PRIVACY AND WHAT THEY CAN DO BETTER 18 (2024), https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf [https://perma.cc/S5KK-BGS3].

[307] Terri Gerstein, *The Role of State Attorneys General in Protecting Workers' Rights*, AM. CONST. SOC'Y: ACS BLOGS (Sep. 4, 2022), https://www.acslaw.org/expertforum/the-role-of-state-attorneys-general-in-protecting-workers-rights/ [https://perma.cc/D9CU-PA6Q] (examining resource constraints that limit state attorneys general offices' ability to effectively enforce laws).

[308] *See id.*

[309] FITZGERALD, WILLIAMS & CROSS, *supra* note 306.

Another notably problematic area is negligent database security practices that lead to unauthorized breaches. Despite the increasing frequency and severity of data breaches—with over 3,205 publicly reported breaches in 2023 exposing 1.7 billion consumer records[310]—current regulatory frameworks provide inadequate incentives for businesses to implement robust security measures.[311] While several high-profile breaches have resulted in substantial settlements, including Capital One's $190 million settlement for its 2019 breach affecting 100 million consumers,[312] and T-Mobile's $350 million settlement for its 2021 breach exposing 76.6 million records,[313] these amounts remain insufficient when compared to the costs of implementing comprehensive security programs.[314] Moreover, the fragmented nature of current regulations creates confusion about security standards, with different states imposing varying requirements for what constitutes "reasonable" security measures.[315] Regulatory uncertainty combined with insufficient penalties has led to a business environment where many choose the risk of a breach over investing in adequate preventative measures.

Perhaps more concerning is the ineffective deterrence created by current penalty structures. Even when violations result in successful enforcement actions, the ultimate penalties generally represent mere fractions of the violating companies' revenues. For example, the CCPA's penalties are capped at $7,500 per intentional violation, which pales in comparison to the GDPR's potential fines of up to four percent of global annual revenue.[316] Or consider the highly publicized $725 million settlement Meta paid in response to privacy violations from the Cambridge Analytica scandal.[317] While

---

[310] IDENTITY THEFT RES. CTR., 2023 DATA BREACH REPORT, https://www.idtheftcenter.org/publication/2023-data-breach-report/ [https://perma.cc/TW5B-VW4Q] (last visited Jan. 18, 2025).

[311] *See supra* Section II.A (discussing the penalty structures of current privacy regulation).

[312] Dan Avery, *Capital One $190 Million Data Breach Settlement: Today Is the Last Day to Claim Money,* CNET (Sep. 30, 2022, at 08:54 PT), https://www.cnet.com/personal-finance/capital-one-190-million-data-breach-settlement-today-is-deadline-to-file-claim/ [https://perma.cc/FSJ2-9ZKG].

[313] Dan Avery, *Deadline Passes on T-Mobile's $350 Million Settlement Days After Another Data Breach,* CNET (Jan. 24, 2023, at 10:00 PT), https://www.cnet.com/personal-finance/deadline-passes-on-t-mobiles-350-million-settlement-days-after-another-data-breach/ [https://perma.cc/RYN7-DSDV].

[314] *See* IBM, COST OF A DATA BREACH REPORT 2024 4 (2024), https://www.ibm.com/reports/data-breach [https://perma.cc/NE8S-93VU] (finding average cost of implementing comprehensive security measures exceeds $4.88 million annually).

[315] *See* William McGeveran, *The Duty of Data Security*, 103 MINN. L. REV. 1135, 1153–54 (2019) (analyzing divergent approaches to "reasonable security" requirements across state laws).

[316] *Compare* CCPA § 1798.155(b), *with* GDPR, art. 83 (demonstrating the significant disparity between CCPA's $7,500 maximum penalty per intentional violation and GDPR's fines of up to 4% of global annual revenue).

[317] Arjun Kharpal, *Facebook Parent Meta Agrees to Pay $725 Million to Settle Privacy Lawsuit*, CNBC (Dec. 23, 2022, at 04:47 ET), https://www.cnbc.com/2022/12/23/facebook-parent-meta-agrees-to-pay-725-million-to-settle-privacy-lawsuit-prompted-by-cambridge-analytica-scandal.html [https://perma.cc/YTE9-J37A].

historically large, it represented less than 0.5 percent of the company's annual revenue.[318] Critics have described this as an ineffective algebra of deterrence,[319] where businesses weigh the potential penalties and probability of getting caught against expected profits and rationally decide to continue violating data privacy. Like risking a $5 parking ticket for a parking spot that will otherwise cost you $100, the current penalty framework fails to create meaningful incentives for compliance, leading to the pervading view that fines are just another cost of doing business.

Inconsistent compliance requirements represent another issue area of the current patchwork approach, as businesses are forced to navigate a proverbial regulatory minefield. While many state privacy laws share common elements, they differ significantly in crucial details, such as how they define personal information and what constitutes a sale of data.[320] Affecting nearly all businesses that participate in the digital economy—either directly through compliance obligations or indirectly through contractual requirements from larger partners—these regulatory variations present particular challenges for small and medium-sized businesses that often lack the resources to implement state-specific compliance programs.[321] Furthermore, this framework creates unintended advantages for larger firms, which can leverage their superior resources to manage compliance costs more effectively.[322]

Critics have suggested that many of these enforcement and compliance issues would be reduced with the passage of federal data privacy laws that supersede the current patchwork of state laws,[323] citing the GDPR's effectiveness at providing businesses with uniform compliance obligations and more stringent penalties.[324] However, this argument overlooks the risk that a superseding federal law is more vulnerable to targeted lobbying efforts that have historically weakened enforcement mechanisms in other industry-wide regulations, such as Dodd-Frank's

---

[318] *See* META PLATFORMS, INC., META REPORTS FOURTH QUARTER AND FULL YEAR 2022 RESULTS 1 (2023), https://s21.q4cdn.com/399680738/files/doc_financials/2022/q4/Meta-12.31.2022-Exhibit-99.1-FINAL.pdf [https://perma.cc/G59F-7XZ2].

[319] *See* Kara Swisher, *Put Another Zero on Facebook's Fine: Then We Can Talk.*, N.Y. TIMES (Apr. 25, 2019), https://www.nytimes.com/2019/04/25/opinion/facebook-fine.html [https://perma.cc/4JYS-H7HP].

[320] *Compare* CCPA § 1798.140(v) (defining personal information to include inferences drawn from other personal information), *with* VA. CODE ANN. § 59.1-575 (adopting a narrower definition of personal information).

[321] Daniel Castro, Luke Dascoli & Gillian Diebold, *The Looming Cost of a Patchwork of State Privacy Laws*, INFO. TECH. & INNOVATION FOUND. (Jan. 24, 2022), https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/ [https://perma.cc/JG6H-SLFK].

[322] *See id.*

[323] Lammonds, *supra* note 224, at 112 (arguing that a unified federal privacy standard would reduce compliance burdens).

[324] *See id.* at 113–14.

diluted financial reforms[325] or the FCC's repeal of net neutrality protections,[326] ultimately leaving consumers less protected.

3. Regulatory Gaps in the Secondary Market

The secondary market for consumer data represents a significant blind spot in the current regulatory framework. While the CCPA-modeled patchwork of state laws establishes basic rules for initial data collection, they largely fail to adequately address the data supply chain and brokers who aggregate, analyze, and resell data after its initial capture.[327]

Data brokers operate with minimal oversight in most jurisdictions, with the majority of state data privacy laws failing to directly regulate them.[328] The few states that have enacted laws to directly regulate brokers provide only limited oversight.[329] For example, Vermont and California require that brokers register with state agencies, pay a small annual fee, and provide minimal disclosures about data collection practices and opt-out procedures.[330] These limited mechanisms fall short of providing substantive consumer protections or transparency over data collection and resale practices.[331]

Additionally, the opacity of the data supply chain presents significant challenges for both businesses and consumers. Businesses purchasing data lack visibility into data's origin and quality because no U.S. privacy law currently requires comprehensive documentation of data lineage or verification of compliance throughout the data supply chain.[332] This creates added risk for businesses that base critical decisions about marketing campaigns, product development, and pricing strategies on data of unknown quality or origin.[333]

For consumers, this lack of transparency of data flow throughout the secondary market nullifies their ability to maintain control over their personal

---

[325] Arthur E. Wilmarth, Jr., *The Dodd-Frank Act: A Flawed and Inadequate Response to the Too-Big-to-Fail Problem*, 89 OR. L. REV. 951, 954–56 (2011) (analyzing how industry lobbying significantly weakened Dodd-Frank's initial regulatory proposals).

[326] *See* AJ Dellinger, *Here's How Telecom Giants Spent More Than $1 Billion Lobbying Congress*, FORBES (May 31, 2019, at 21:52 ET), https://www.forbes.com/sites/ajdellinger/2019/05/31/heres-how-telecom-giants-spent-more-than-1-billion-lobbying-congress/ [https://perma.cc/7J9X-NUJS] (analyzing how industry lobbying influenced the FCC's reversal of net neutrality protections).

[327] *See* FITZGERALD, WILLIAMS & CROSS, *supra* note 306.

[328] COLO. REV. STAT. § 6-1-1301; UTAH CODE ANN. § 13-61-101; *see* VA. CODE ANN. § 59.1-575.

[329] CCPA § 1798.99.80; *see* VT. STAT. ANN. tit. 9, § 2446 (2018).

[330] *See* VT. STAT. ANN. tit. 9, § 2446(a)(1)–(5) (requiring annual registration, $100 fee, and basic disclosures); *see also* CCPA § 1798.99.82(b)(1)–(4) (mandating annual registration, $400 fee, and general disclosures).

[331] CCPA § 1798.99.82(b)(1)-(4); *see* VT. STAT. ANN. tit. 9, § 2446(a)(1)-(5).

[332] *See* FITZGERALD, WILLIAMS & CROSS, *supra* note 306.

[333] *See How Data Chaos Undermines Your Business Success*, *supra* note 43.

information. While privacy policies govern initial data collection, these agreements rarely cover subsequent data transfers, permitting downstream data usage to extend far beyond the scope of what consumers initially agreed to or could reasonably foresee.[334] State regulations primarily focus on the point of initial collection, largely omitting subsequent transfers and uses.[335] For example, the CCPA's right to know provision requires businesses to disclose data-sharing practices,[336] but by requiring only superficial disclosure of the initial data transfer, this requirement fails to account for the multilayered and opaque nature of how data actually flows through the supply chain. This gap in oversight has left consumers with minimal transparency into or recourse to address the unconstrained flow of their personal information.[337]

Collectively, these critiques highlight some of the fundamental issues with the current patchwork approach to consumer data regulation. From the perfunctory nature of Notice and Consent to the inadequate enforcement mechanisms used by states and the compliance challenges they create, to the regulatory gaps in the secondary market, these systemic weaknesses illustrate how ineffective the current regulatory approach is at addressing the evolving challenges of data privacy. While these realizations have led many to advocate for more comprehensive and uniform data privacy laws, the following Section demonstrates why this common conclusion is impractical.

A. The Impracticality of Federal Legislative Solutions

In response to the systemic issues that pervade the current privacy landscape, many privacy advocates and lawmakers have pushed for comprehensive federal legislation modeled after GDPR and CCPA.[338] These proposals typically aim to impose greater accountability and transparency requirements on businesses while providing consumers with

---

[334] *See* FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY 47–49 (2014) https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/6ZB4-XN33].

[335] *See Data Privacy Laws: What You Need to Know in 2025*, OSANO (Sep. 26, 2025), https://www.osano.com/articles/data-privacy-laws [https://perma.cc/QZ8U-Z39L] (surveying state privacy laws and highlighting focus on initial collection and disclosure rather than data transfers).

[336] *See* CCPA § 1798.110(a)(2)–(4) (requiring only disclosure of categories of sources, third parties, and sharing practices).

[337] *See* Rex Chen et al., *Fighting the Fog: Evaluating the Clarity of Privacy Disclosures in the Age of CCPA*, ARXIV, at 1 (Sept. 28, 2021), https://arxiv.org/pdf/2109.13816 [https://perma.cc/Y9Z5-LKA3].

[338] Caitlin Chin-Rothmann, *Highlights: The GDPR and CCPA as Benchmarks for Federal Privacy Legislation*, BROOKINGS INST. (Dec. 19, 2019), https://www.brookings.edu/articles/highlights-the-gdpr-and-ccpa-as-benchmarks-for-federal-privacy-legislation/ [https://perma.cc/DGJ2-HUZK].

foundational privacy rights.[339] Proponents argue that federal legislation would resolve compliance challenges created by the current state law patchwork, establish consistent baseline protections, and enable more effective enforcement through empowered federal agencies.[340] The successful implementation of GDPR across Europe and recent polling showing 82 percent of Americans have security concerns about online data and 84 percent support strict federal data privacy legislation[341] seemingly validate this approach. However, this seemingly intuitive solution proves impractical when accounting for the realities of the American digital economy, where social, political, and market forces act as preventative barriers to meaningful federal privacy regulation.[342]

1. Social Forces: The Privacy Paradox and Consumer Behavior

An examination of social forces reveals the fundamental contradiction between consumers' stated privacy preferences and observed marketplace behavior. Despite expressed concerns about data privacy, consumers consistently demonstrate an unwillingness to pay the monetary costs for digital services, preferring instead to exchange their personal data as currency.[343] As discussed in the Introduction, this demonstrated preference has organically helped fuel the advertising-based business models that dominate the modern internet, in which consumers' attention and data are monetized rather than the services themselves.[344]

This disparity between stated preferences about privacy and actual behavior, known as the Privacy Paradox, presents a significant challenge to implementing effective privacy legislation.[345] While polling indicates strong public bipartisan support for privacy protections,[346] consumer behavior tells a different story. When presented with privacy-forward alternatives to popular services, consumers consistently choose the privacy-invasive options.[347] For example, compare the most prolific privacy-forward search engine, DuckDuckGo, capturing less than one percent global market share,

---

[339] *See id.*
[340] *See id.*
[341] Rob Lever, *Data Privacy Paradox: A Survey of Americans' Online Security Top Concerns & Problematic Habits*, U.S. NEWS & WORLD REP. (Aug. 5, 2024, at 10:00 ET), https://www.usnews.com/360-reviews/privacy/digital-privacy-concerns-habits-survey [https://perma.cc/679U-G3AL].
[342] *See* discussion *supra* Introduction.
[343] *See* discussion *supra* Introduction.
[344] *See* discussion *supra* Introduction.
[345] Perla Khattar, *What You Don't Know Will Hurt You: Fighting the Privacy Paradox By Designing for Privacy and Enforcing Protective Technology*, 18 WASH. J. L. TECH. & ARTS 1, 2 (2023).
[346] *See* McClain et al., *supra* note 264.
[347] *See* Khattar, *supra* note 345.

with Google's 82 percent.[348] Empirical studies have also validated this behavioral contradiction, demonstrating that consumers overwhelmingly value price over privacy implications when choosing between services.[349]

This paradoxical behavior is further exacerbated by society's growing technological dependence and addiction.[350] From connecting with friends and family, to dating, to working, to making dinner, digital services have transcended mere convenience to become essential for social and economic participation.[351] Americans spend an average of seven hours per day on internet-connected devices,[352] compulsively checking their phones an average of 205 times per day.[353] For many, this relationship has transcended beyond dependence and into full-scale addiction.[354] For example, TikTok has proven so engaging that worldwide users spend an average of 95 minutes per day on the app.[355] This technological dependence helps explain why federal legislators remain trepidatious about supporting privacy legislation that interferes with this system of data-subsidized services that consumers demand.[356]

Given this dynamic, the Privacy Paradox underscores how futile reforming the Notice and Consent framework would be.[357] While appealing in theory, such reforms are nonviable given the public's insatiable hunger for low-cost technology and how deeply ingrained the exchange of data for services is in modern digital life. Any regulatory framework purporting to give consumers meaningful control over their data would be illusory at best—not only because of demonstrated consumer preferences to pay with data over money, but because too much consumer data has already flooded the market with

---

[348] *Market Share of Leading Desktop Search Engines Worldwide from January 2015 to October 2025*, *supra* note 291.

[349] *See* Alastair R. Beresford, Dorothea Kübler & Sören Preibusch, *Unwillingness to Pay for Privacy: A Field Experiment*, 117 ECON. LETTERS 25, 27 (2012) (finding that when offered identical products with different privacy protections, consumers almost always choose the cheaper option regardless of privacy implications).

[350] *See, e.g.*, Trevor Wheelwright, *Cell Phone Usage Stats 2026: Americans Check Their Phones 205 Times a Day*, REVIEWS.ORG (Jan. 1, 2025), https://www.reviews.org/mobile/cell-phone-addiction/ [https://perma.cc/ESY3-BR3W].

[351] *See generally* COMMON SENSE MEDIA, THE COMMON SENSE CENSUS: MEDIA USE BY TWEENS AND TEENS (2021), https://www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf [https://perma.cc/2ZT4-Q8VU] (showing how media and technology are integral to the lives of Tweens and Teens).

[352] Lindsey Leake, *17 Years of Your Adult Life May Be Spent Online. These Expert Tips May Help Curb Your Screen Time.*, FORTUNE (Mar. 6, 2024, at 05:10 ET), https://fortune.com/well/article/screen-time-over-lifespan/ [https://perma.cc/G4TH-AQNG].

[353] Wheelwright, *supra* note 350.

[354] *See id.* (discussing the self-reported rates of cell phone addiction).

[355] *TikTok Statistics You Need to Know*, BACKLINKO (Nov. 19, 2025), https://backlinko.com/tiktok-users [https://perma.cc/PBQ4-XCNN].

[356] *See* Amy Howe, *Supreme Court Upholds TikTok Ban,* SCOTUSBLOG (Jan. 17, 2025, at 12:45 ET), https://www.scotusblog.com/2025/01/supreme-court-upholds-tiktok-ban/ [https://perma.cc/4X25-LWVH].

[357] *See supra* Section II.B.1 (analyzing fundamental failures of Notice and Consent framework).

businesses dependent on its continued collection and use.[358] These realities render alternative privacy-protective frameworks impractical.

2. Political Forces: Barriers to Comprehensive Regulation

The current political landscape poses additional barriers to federal privacy legislation, especially in the post-Citizens United era, where corporate influence over the legislative process has expanded dramatically.[359] The 2010 Supreme Court decision effectively removed limits on campaign finance, enabling corporations and wealthy individuals to wield outsized influence through lobbying efforts and political contributions.[360] This shift has created an environment where lawmakers are increasingly beholden to special interests with substantial financial resources.[361]

In this environment, Big Tech's deep pockets have proven particularly influential at perpetuating legislative deadlock. Industry lobbying spend in recent years has hovered around $100 million per year, with companies like Meta, Amazon, and Alphabet making up the bulk of those expenditures.[362] Campaign contributions have also exploded, ranging from $45 to $98 million per election cycle.[363] This led to demonstrable results, with none of the federal attempts at comprehensive data privacy legislation passing in either chamber of Congress.[364]

In addition to corporate lobbying, the influence of individual tech executives has raised new concerns. For example, President Trump's inauguration fund raised over $200 million, including $1 million in donations from the chairmen/CEO's of Uber, Meta, Apple, Amazon, and OpenAI.[365] Such donations suggest an expectation of preferential treatment, further eroding public trust in the legislative process. Perhaps the most concerning illustration of this is X/Twitter owner Elon Musk's $277 million in support of Donald Trump and Republican candidates.[366] Following these

---

[358] *See supra* Section I.C (examining the extent of data collection practices and business dependencies).
[359] *See* Daniel I. Weiner, *Citizens United, Explained*, BRENNAN CTR. FOR JUST. (Jan. 29, 2025), https://www.brennancenter.org/our-work/research-reports/citizens-united-explained [https://perma.cc/Z5DM-EBKM].
[360] *Id.*
[361] *Id.*
[362] *Industry Profile: Internet*, OPENSECRETS (2024), https://www.opensecrets.org/federal-lobbying/industries/summary?cycle=2024&id=B13 [https://perma.cc/H762-FANQ].
[363] *Id.*
[364] *See* discussion *supra* Section II.A.4.
[365] *Big Tech Is Donating Millions to Trump's Inauguration*, COMMON CAUSE: BLOG POST (Jan. 10, 2025), https://www.commoncause.org/articles/big-tech-is-donating-millions-to-trumps-inauguration/ [https://perma.cc/Z6HX-83DJ].
[366] Josh Marcus, *Elon Musk's Wealth Jumps By $170bn Since Election After He Backed Trump with $277m*, INDEPENDENT (Dec. 16, 2024, at 17:40 ET), https://www.the-

contributions, the market priced in Musk's newfound political influence with a $170 billion increase to his net worth,[367] highlighting the symbiotic relationship between political contributions, market valuations, and regulatory outcomes in today's era of crony capitalism.

As recent events surrounding the attempted TikTok ban illustrate, the tools of Big Tech's political influence go beyond financial contributions to include the power to manipulate public perception to the point of affecting policy outcomes.[368] Despite valid national security concerns that led the Supreme Court to uphold the law banning the Chinese social media app,[369] President Trump signed an executive order delaying the ban by 75 days after millions of "TikTok refugees" took to social media in protest.[370] Many even went so far as to join Rednote, a more privacy-invasive Chinese app.[371] Since then, Trump has repeatedly extended the forced sale deadline, most recently in June 2025, marking the third such extension, demonstrating both the difficulty of enforcing restrictions on a platform so culturally embedded and the political costs of confronting it directly.[372] Beyond showcasing how deeply rooted social media's influence is over American youth,[373] this event showed how Big Tech's political influence extends across party lines.[374] Both Republican and Democratic lawmakers—including California Rep. Ro Khanna, New Jersey Sen. Corey Booker, and Kentucky Sen. Ron Paul—supported efforts to repeal this ban, highlighting the systemic nature of this issue as resistance to sensible tech

---

independent.com/news/world/americas/elon-musk-net-worth-trump-b2665395.html [https://perma.cc/7WJT-HGEQ].

[367] *Id.*

[368] *See* Howe, *supra* note 356.

[369] *Id.*

[370] *See* Julia Shapero & Miranda Nazzaro, *Trump Faces TikTok Backlash*, HILL (Jan. 21, 2025, at 17:24 ET), https://thehill.com/newsletters/technology/5098943-trump-faces-tiktok-backlash/ [https://perma.cc/9ABQ-36FE].

[371] Katie Paul, *Chinese App RedNote Gains Millions of U.S. Users This Week as 'TikTok Refugees' Joined Ahead of Ban*, REUTERS (Jan. 16, 2025, at 19:34 ET), https://www.reuters.com/technology/chinese-app-rednote-gained-millions-us-users-this-week-tiktok-refugees-joined-2025-01-16/ [https://perma.cc/8WX5-7ENN].

[372] John Ruwitch, *Trump Pushes Back TikTok's Sell-By Date for a Third Time*, NPR (June 19, 2025, at 12:18 ET), https://www.npr.org/2025/06/18/nx-s1-5430884/trump-tiktok-ban-third-extension [https://perma.cc/ 8QJS-XRSB].

[373] *See* Shapero & Nazzaro, *supra* note 370.

[374] *See* Press Release from Rep. Ro Khanna, Rep. Ro Khanna & Dr. Rand Paul Introduce Bipartisan, Bicameral Repeal the TikTok Ban (Jan. 24, 2025) [hereinafter Rep. Ro Khanna & Dr. Rand Paul], https://khanna.house.gov/media/press-releases/rep-ro-khanna-and-dr-rand-paul-introduce-bipartisan-bicameral-repeal-tiktok [https://perma.cc/MME8-WK75]; Press Release from Rep. Ro Khanna, Rep. Khanna & Senators Markey, Wyden, & Booker Announce Legislation to Extend TikTok Ban Deadline (Jan. 14, 2025) [hereinafter Rep. Khanna & Senators], https://khanna.house.gov/media/press-releases/rep-khanna-senators-markey-wyden-and-booker-announce-legislation-extend-tiktok [https://perma.cc/Z9FD-E6EJ].

regulation has passed the seemingly insurmountable bipartisan threshold.[375]

3. Market Forces: Dependencies on Consumer Data

Among these barriers to meaningful privacy regulation, market forces present perhaps the most formidable challenge. The digital economy has developed deep structural dependencies on consumer data, making significant change more unlikely than ever.[376] The advertising-based business models that emerged as part of the internet's "original sin" have shaped the modern digital economy, where businesses exchange free services for consumer data and attention, which are ultimately monetized through targeted advertising.[377] Any privacy law that interferes with this dynamic to the point of reducing business revenue would likely lead to a degradation of services or increased costs passed on to consumers, forcing some companies to restructure their nonviable business models.[378]

This reliance on consumer data extends far beyond Big Tech to the broader business community, with modern companies increasingly dependent on consumer data to compete effectively.[379] From optimizing pricing strategies and inventory management to personalizing customer experiences and identifying market trends, consumer data is a strategic asset that businesses across all sectors rely on to make informed strategic decisions.[380] Any comprehensive regulation would therefore detrimentally impact businesses market-wide.

Moreover, innovation would similarly be affected by comprehensive privacy regulation. Restricted access to consumer data would delay tech production cycles by limiting companies' ability to identify user needs, test new features, and measure product improvement efficacy.[381] For start-ups

---

[375] *See* Rep. Ro Khanna & Dr. Rand Paul, *supra* note 374; Rep. Khanna & Senators, *supra* note 374.

[376] *See* Daron Acemoglu et al., *Online Business Models, Digital Ads, and User Welfare* 12–15 (MIT DEP'T OF ECON., Working Paper No. 2024-09, 2024), https://economics.mit.edu/sites/default/files/2024-09/Online%20Business%20Models%2C%20Digital%20Ads%2C%20and%20User%20Welfare.pdf [https://perma.cc/Z32X-PHEX] (examining how the digital economy's structural dependency on advertising revenue creates significant barriers to privacy regulation, as meaningful restrictions would force companies to either degrade services or shift costs to consumers).

[377] *See* discussion *supra* Introduction.

[378] *See* Sarah Kuta, *Data Privacy Laws May Cost Companies Billions*, CHI. BOOTH REV. (Apr. 13, 2023), https://www.chicagobooth.edu/review/data-privacy-laws-may-cost-companies-billions [https://perma.cc/Z6N3-AHNQ] (analyzing how privacy regulations that restrict data collection could force companies to either implement paid service models or significantly reduce service quality to maintain profitability).

[379] *See id.*

[380] *See supra* Section I.A (discussing how consumer data has become a requisite commodity for modern business operations); *see also supra* Section II.C (examining how individual companies have grown dependent on consumer data for strategic decision-making).

[381] *See supra* Section I.D.1 (discussing how companies use consumer data to make strategic decisions about product development and optimization).

and emerging companies, these limitations could prove especially detrimental, as reduced access to third-party data and increased compliance costs would create substantial barriers to entry.[382] Such barriers would inadvertently strengthen the market position of larger companies, which possess the resources to both comply with more stringent regulations and maintain the massive proprietary datasets needed to develop new products.[383] Furthermore, a more adversarial regulatory environment would likely lead R&D focused companies to reallocate their operations to a more friendly regulatory environment, diminishing America's position as a global innovation leader.[384]

These existing market barriers have become more deeply entrenched with the emergence of AI, transforming data from an important business asset into a requisite strategic resource that necessitates relaxed data privacy laws.[385] The development of AI models depends on access to vast quantities of high-quality training data.[386] Historical user data is uniquely suited for this because it possesses the complexities of authentic human behavior that cannot be synthetically replicated.[387] Relaxed federal privacy laws are therefore required to keep consumer data flowing if the rapid development of AI capabilities is to continue.[388]

Beyond demonstrating consumer data's importance to AI models, this dynamic helps explain why Big Tech has collectively made such an unprecedented bet on AI infrastructure, creating a $600 billion hole in annual revenue that will need to be filled.[389] With a transformational technology on the horizon and a competitive moat built from years of consumer data and hundreds of billions of dollars in infrastructure investment, Big Tech took this calculated risk and went all in on AI.[390] Following the proven model of search engines and social networks, AI presents another opportunity to monetize consumer attention and

---

[382] *See generally* James Campbell, Avi Goldfarb & Catherine Tucker, *Privacy Regulation and Market Structure*, 24 J. ECON. & MGMT. STRATEGY 47 (2015) (arguing that general privacy rules favor larger companies).

[383] *See generally id.* (analyzing how data access barriers create competitive advantages for incumbent firms).

[384] *See, e.g.*, *Business Relocation: 8 Key Factors to Consider Before You Move*, BPM (Dec. 20, 2024), https://www.bpm.com/insights/business-relocation/ [https://perma.cc/DDA7-ECL7] (analyzing how increasing regulatory burdens in certain jurisdictions drive businesses to relocate operations to more favorable regulatory environments, particularly in R&D-intensive sectors).

[385] *See supra* Section I.C.1 (discussing Big Tech's use of consumer data for AI model training).

[386] *See supra* Section I.C.1.

[387] Lauren Leffer, *Your Personal Information Is Probably Being Used to Train Generative AI Models*, SCI. AM. (Oct. 19, 2023), https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/ [https://perma.cc/FHG8-3YTR] (explaining how AI models require real-world user data to develop a genuine understanding of human behavior and communication patterns that synthetic data cannot replicate).

[388] *See id.*

[389] *See supra* Section I.D.2 (discussing $600 billion in annual revenue required to break even).

[390] *See supra* Section I.D.2.

predicted behavior through advertising, provided that it can continue to attract, retain, and profile consumers.[391]

Therefore, the answer to the $600 billion question posed at the end of Part I can be inferred from these collective social, political, and market forces. Big Tech's massive investment suggests absolute confidence that comprehensive privacy regulation is not on the horizon, as the steady flow of consumer data and lax regulatory environment are required to effectively develop and monetize next-generation AI platforms.[392]

In sum, Part II has demonstrated how the current regulatory landscape, despite its continued incremental progress, remains inadequate at addressing the evolving challenges of modern data privacy. The combined structural flaws of Notice and Consent, impotent enforcement mechanisms, and regulatory gaps of the secondary market have produced a system that's left consumers with limited protections and businesses with complex compliance challenges.[393] Moreover, the collective social, political, and market forces make comprehensive federal legislation more impractical than ever.[394] Given these realities, Part III proposes an alternative path forward that accepts certain privacy limitations while expanding liability frameworks to address substantial harms.

III. ACCEPTANCE AND A PRAGMATIC APPROACH TO DATA PRIVACY

In reaction to these systemic problems of consumer data privacy laws, many critics and legal scholars have proposed the same general solution of comprehensive federal legislation.[395] This Part advocates for an alternative path forward: first, arguing for the acceptance of the current weak regulatory environment as the logical trade-off for the modern digital economy; then, by proposing an expansion of existing liability frameworks for substantial harms. This approach accepts the necessary role consumer data plays in modern digital life, yet seeks to hold companies to account for harms attributable to data misuse.

A. Accepting Limited Privacy as the Cost of Innovation

Rather than pursuing comprehensive federal privacy legislation that appears increasingly unlikely to have a meaningful impact on the issues previously discussed, this Note advocates for accepting the current state of

---

[391] *See supra* Section I.C.1 (discussing the business model favored by Big Tech).
[392] *See* Cahn, *supra* note 151 (examining how Big Tech's unprecedented AI investments indicate their expectation of minimal privacy regulation impeding data collection for AI development).
[393] *See supra* Section II.B.
[394] *See supra* Section II.C.
[395] *See* Lammonds, *supra* note 224, at 112.

limited privacy protections as a logical trade-off for continued access to innovative technologies. As detailed throughout this Note, the digital economy has evolved to where consumer data serves as the primary currency, enabling technological innovation.[396] From the "original sin" of choosing advertising-based monetization to the modern AI arms race, this system has produced unprecedented technological advancement while making cutting-edge services universally accessible.[397] The demonstrated consumer preference for convenience and free services over privacy protections, coupled with society's growing technological dependence, has created a marketplace where meaningful data privacy is fundamentally incompatible with continued access to the services consumers demand.[398]

Moreover, acceptance aligns with the economic realities, as the massive infrastructure investments made by Big Tech—particularly in AI development—necessitate continued access to consumer data for both development and monetization.[399] With companies collectively betting hundreds of billions on AI infrastructure,[400] any meaningful privacy regulation would threaten not just current business models but future innovation.[401] Given these market dynamics, technological dependencies, and demonstrated consumer preferences, accepting diminished personal privacy and weak data privacy laws is the fair market value for maintaining the pace of innovation and universal access to transformative technologies. However, acceptance does not have to mean a complete acquiescence to Big Tech's agenda. Instead, acceptance should be accompanied by an expanded framework of liability that provides effective recourse for substantial harms caused by data misuse.

B. An Expanded Framework for Data Privacy Liability

Drawing from the known and foreseeable misuses of consumer data previously discussed, this framework would focus on three key areas of liability: (1) negligent data security practices leading to unauthorized access; (2) the unauthorized sharing, sale, or use of sensitive personal information; and (3) algorithmic decision making that causes concrete harm.[402] This targeted approach addresses the most harmful practices

---

[396] *See supra* Section I.A.
[397] *See supra* Introduction (discussing the progression of the data economy in general terms).
[398] *See supra* Section II.C.1 (discussing the privacy paradox).
[399] *See supra* Section I.D.2.
[400] *See, e.g.*, Ari Levy, *Tech's $380 Billion Splurge: This Quarter's Winners and Losers of the AI Spending Boom*, CNBC (Oct. 31, 2025, at 11:13 ET), https://www.cnbc.com/2025/10/31/tech-ai-google-meta-amazon-microsoft-spend.html [https://perma.cc/H5NS-YGW4].
[401] *See supra* Section II.C.3 (discussing the detrimental effects privacy regulation would have on innovation).
[402] *See supra* Section I.D (examining potential harmful applications of consumer data).

while avoiding the broad, disruptive effect on consumer experience and business function that an overinclusive prophylactic regulation would have.

A critical challenge under the current legal framework is the difficulty consumers face in discovering privacy violations, as many harmful practices occur behind proprietary walls with limited transparency.[403] To address this information asymmetry, this framework should incorporate expanded whistleblower protections and incentives similar to those that have proven effective in other regulatory contexts. For example, following the model of the False Claims Act, a qui tam provision would incentivize insiders to report violations by granting them a percentage of any resulting settlement, creating effective financial rewards for the disclosure of harmful practices that might otherwise remain hidden.[404]

Beyond empowering whistleblowers, this framework would establish a blanket private right of action and provide for uncapped damages for privacy violations. As demonstrated by BIPA's success, private rights of action serve both to provide meaningful recourse for harmed consumers and create effective deterrence through the threat of significant damages.[405] Unlike the current patchwork of state laws, which rely primarily on resource-constrained state agencies for enforcement, this approach would leverage additional resources from the private sector to identify and pursue violations.[406] Additionally, damages should be uncapped to allow penalties to scale with company size and violation severity, and ensure harmed parties are made whole. The combination of whistleblower incentives, expanded litigation rights, and uncapped damages would provide for more robust enforcement mechanisms to effectively deter potential violators.

Moreover, this framework would increase compliance throughout the data ecosystem because liability for non-permitted use would follow the data along the entire supply chain. Big Tech, data brokers, and all secondary market participants would assume greater accountability for data collection, custody, and use due to this expanded risk of liability from uncapped penalties, whistleblowers, and private civil actions.

---

[403] *See generally* U.S. GOV'T ACCOUNTABILITY OFF., GAO-22-106096, CONSUMER DATA: INCREASING USE POSES RISK TO PRIVACY (2022), https://www.gao.gov/products/gao-22-106096 [https://perma.cc/6VF2-2JLA] (analyzing how lack of transparency and information asymmetries prevent consumers from identifying privacy violations and recommending expanded whistleblower protections to enhance oversight).

[404] *See* 31 U.S.C. § 3730(d) (2018) (providing that qui tam relators can receive between fifteen and thirty percent of the proceeds of the action or settlement).

[405] *See supra* Section II.A.2 (discussing BIPA's private right of action and resulting settlements).

[406] *See generally* Adam Schwartz, *You Should Have a Private Right of Action to Sue Companies that Violate Your Privacy*, ELEC. FRONTIER FOUND. (Jan. 7, 2019), https://www.eff.org/deeplinks/2019/01/you-should-have-right-sue-companies-violate-your-privacy [https://perma.cc/6R9P-WNF4] (advocating for private right of action to supplement limited state enforcement resources and increase detection of privacy violations).

For this framework to be effective, it must be implemented at the federal level and preempt the patchwork of state laws. As discussed in Part II, the borderless nature of how data flows throughout the digital economy makes the patchwork approach to regulation both ineffective and unnecessarily burdensome for businesses.[407] A single, unified federal framework would eliminate these jurisdictional issues while ensuring consistent consumer protections nationwide. Furthermore, because the prospect of passing a standalone data privacy law remains unlikely at best, any expansion of liability should be passed as an addendum to unrelated federal legislation, such as an appropriations bill.

Collectively, this approach provides a measured solution that allows consumers to maintain their privacy-subsidized access to cutting-edge technologies yet mitigate the threat of substantial harm inherent in this system of ubiquitous data collection. Critics are sure to point out that this solution fails to address the underlying loss of privacy or reform the fundamentally flawed Notice and Consent framework,[408] but such criticisms disregard the practical reality that true data privacy is incompatible with the modern digital economy. Rather than pursuing illusory reforms that promise consumers control they can never meaningfully exercise, this solution provides a pragmatic balance that accepts privacy as the cost of technological progress without completely acquiescing to Big Tech.

IV. CONCLUSION

The rapid emergence of consumer data's use throughout the modern digital economy[409] has transformed the relationship between consumers and technology companies, creating a dynamic where consumer data has become the de facto currency of the digital age. While growing public awareness of data collection practices has amplified calls for stronger privacy protections, this Note argues that such reforms are both impractical and undesirable given the realities of our modern digital economy.[410] The combination of consumers' demonstrated preference for free services over privacy, society's growing dependence and addiction to technology, and businesses' reliance on consumer data for competition and innovation—particularly in emerging fields like AI—has created a marketplace where meaningful data privacy protections are

[407] *See supra* Section II.B.2 (discussing compliance challenges created by state privacy law patchwork).
[408] *See* discussion *supra* Part I (discussing the inefficacy of the Notice and Consent framework).
[409] *See supra* Introduction (discussing the evolution of the modern digital economy).
[410] *See supra* Section II.B (analyzing failures of current privacy protection frameworks).

fundamentally incompatible with continued access to cutting-edge technology.[411]

However, this acceptance of weak privacy protections should not mean a complete acquiescence to Big Tech's agenda.[412] Rather than supporting the continued pursuit of comprehensive privacy legislation that appears increasingly unlikely to have a meaningful impact, this Note advocates for an expanded federal liability framework focused on substantial harms that are concrete and attributable to consumer data misuse.[413] By incorporating robust whistleblower incentives and protections with meaningful private rights of action backed by uncapped damages, this measured approach would maintain the benefits of data-driven innovation while promoting greater accountability throughout the data supply chain.[414] As AI emerges as a transformative technology with a requisite appetite for vast quantities of consumer data,[415] this pragmatic solution becomes not just preferable but necessary to promote a regulatory environment that balances the need for technological innovation with accountable data practices.

---

[411] *See supra* Section II.C (examining social and market barriers to comprehensive privacy regulation).
[412] *See* discussion *supra* Section III.B.
[413] *See* discussion *supra* Section II.B.
[414] *See supra* Section III.B (proposing an expanded federal liability framework as a practical alternative to comprehensive privacy regulation).
[415] *See supra* Section I.C.1 (examining Big Tech's use of consumer data for AI development).